Grayling: Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan

A previously unknown advanced persistent threat (APT) group used custom malware and multiple publicly available tools to target a number of organizations in the manufacturing, IT, and biomedical sectors in Taiwan.

A government agency located in the Pacific Islands, as well as organizations in Vietnam and the U.S., also appear to have been hit as part of this campaign. This activity began in February 2023 and continued until at least May 2023.

The Symantec Threat Hunter Team, part of Broadcom, has attributed this activity to a new group we are calling Grayling. This activity stood out due to the use by Grayling of a distinctive DLL sideloading technique that uses a custom decryptor to deploy payloads. The motivation driving this activity appears to be intelligence gathering.

Attacker Activity

There are indications that Grayling may exploit public facing infrastructure for initial access to victim machines. Web shell deployment was observed on some victim computers prior to DLL sideloading activity taking place. DLL sideloading is used to load a variety of payloads, including Cobalt Strike, NetSpy, and the Havoc framework.

The attackers take various actions once they gain initial access to victims' computers, including escalating privileges, network scanning, and using downloaders.

Tactics, techniques, and procedures (TTPs) used by the attackers included:

- **Havoc:** An open-source post-exploitation command-and-control framework that attackers began using towards the start of 2023, seemingly as an alternative to Cobalt Strike and similar tools. Havoc is able to carry out a variety of activities including executing commands, managing processes, downloading additional payloads, manipulating Windows tokens, and executing shellcode. Havoc is also notable for being cross-platform.
- **Cobalt Strike:** An off-the-shelf tool that can be used to execute commands, inject other processes, elevate current processes, or impersonate other processes, and upload and download files. It ostensibly has legitimate uses as a penetration-testing tool but is invariably exploited by malicious actors.
- **NetSpy:** A publicly available spyware tool.
- **Exploitation of CVE-2019-0803**: An elevation of privilege vulnerability that exists in Windows when the Win32k component fails to properly handle objects in memory.
- **Active Directory discovery:** Used to query Active Directory and help map the network.
- **Mimikatz:** Publicly available credential-dumping tool.
- **Kill processes**
- **Downloaders**
- **Unknown payload** downloaded from imfsb.ini

The typical attack chain in this activity appears to be DLL sideloading through exported API SbieDll_Hook. This leads to the loading of various tools, including a Cobalt Strike Stager that leads to Cobalt Strike Beacon, the Havoc framework, and NetSpy. The attackers were also seen loading and decrypting an unknown payload from imfsb.ini. An exploit for CVE-2019-0803 was also used in the course of this activity, while shellcode was also downloaded and executed.

Other post-exploitation activity performed by these attackers includes using kill processes to kill all processes listed in a file called processlist.txt, and downloading the publicly available credential-dumping tool Mimikatz.

Motivation

While we do not see data being exfiltrated from victim machines, the activity we do see and the tools deployed point to the motivation behind this activity being intelligence gathering. The sectors the victims operate in – manufacturing, IT, biomedical, and government – are also sectors that are most likely to be targeted for intelligence gathering rather than for financial reasons.

The use of custom techniques combined with publicly available tools is typical of the activity we see from APT groups these days, with threat actors often using publicly available or living-off-the-land tools in attempts to bypass security software and help their activity stay under the radar of defenders. Tools like Havoc and Cobalt Strike are also frequently used by attackers due to their wide array of capabilities. It is often easier for even skilled attackers to use existing tools like this than to develop custom tools of their own with similar capabilities. The use of publicly available tools can also make attribution of activity more difficult for investigators. The steps taken by the attackers, such as killing processes etc., also indicate that keeping this activity hidden was a priority for them.

We have not been able to definitively link Grayling to a specific geography, but the heavy targeting of Taiwanese organizations does indicate that they likely operate from a region with a strategic interest in Taiwan.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

File Indicators

SHA256 hashes:

da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9 – Havoc framework
79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17 – Downloader
bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec – Downloader
c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3 – Cobalt Strike Beacon
667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c – Exploit for CVE-2019-0803
87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8 – Downloader
90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0 – Loader
8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2 – Cobalt Strike Stager
d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c – NetSpy
4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba – DLL file
9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739 – NetSpy
f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b – Downloader
525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9 – Downloader
23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae – Downloader
6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50 – Downloader
5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581 – Downloader
12924d7371310c49b1a215019621597926ef3c0b4649352e032a884750fab746 – Windump
ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f

c76ba3eb764706a32013007c147309f0be19efff3e6a172393d72d46631f712e

245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa

4c44efc7d9f4cd71c43c6596c62b91740eb84b7eb9b8cf22c7034b75b5f432d9

e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3

f3e8f2ef4ad949a0ada037f52f4c0e6000d111a4ac813e64138f0ded865e6e31

971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f

f1764f8c6fc428237ffafeb08eb0503558c68c6ccf6f2510a2ef8c574ba347e0

c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5

af26d07754c8d4d1cb88195f7dc53e2e4ebee382c5b84fc54a81ba1cee4d0889

1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce

7ea706d8da9d68e1214e30c6373713da3585df8a337bc64fcc154fc5363f5f1f

30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6

74cbde4d4b4ac4cae943831035bff90814fa54fd21c3a6a6ec16e7e3fb235f87

752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea

6a8c39e4c543e94f6e4901d0facee7793f932cd2351259d8054981cf2b4da814

803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721

7c1b20de1f170cfaf3e75ebc7e81860378e353c84469795a162cd3cfd7263ba2

a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe

de500875266fd18c76959839e8c6b075e4408dcbc0b620f7544f28978b852c1c

1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91

ba8a7af30e02bd45e3570de20777ab7c1eec4797919bfcd39dde681eb69b9faf

1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9

dcadcac4c57df4e31dd7094ae96657f54b22c87233e8277a2c40ba56eafcf548

d0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29

b19ccfa8bc75ce4cf29eb52d4afe79fe7c3819ac08b68bd87b35225a762112ba

6e5d840ddeedc3b691e11a286acd7b6c087a91af27c00044dd1d951da5893068

3acfe90afa3cbb974e219a5ab8a9ee8c933b397d1c1c97d6e12015726b109f1b

5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970

Network Indicators

Domain

d3ktcnc1w6pd1f.cloudfront[.]net

IP addresses

172.245.92[.]207
3.0.93[.]185

URLs

http://45.148.120[.]23:91/version.dll
http://45.148.120[.]23:91/vmtools.exe