Severity: High

Date: 12th Oct 2023

Description

The Grayling threat group, first reported by Symantec in October 2023, has been active since at least February 2023. The group primarily targets organizations in the manufacturing, IT, and biomedical sectors in Taiwan; however, it was also observed targeting a government agency in the Pacific Islands, as well as organizations in the United States and Vietnam.

Methodology

Grayling likely gains initial system access by exploiting public-facing infrastructure. Once inside the system, the threat actors deploy web shells to maintain persistence, and then use DLL sideloading to download various tools, including Cobalt Strike, Net Spy, and the Havoc post-exploitation framework. These tools are used to establish command-and-control (C2) communication, perform network reconnaissance, gather information, and execute arbitrary commands. In addition, Grayling escalates privileges by leveraging a known vulnerability in the Win32k component (CVE-2019-0803). As part of their post-exploitation activities, the threat actors terminate a predetermined list of processes, and dump credentials using Mimikatz. It is believed that Grayling targets organizations for intelligence-gathering purposes rather than for financial reasons.

IOC

URL's

/http://45.148.120.23:91/version.dll/

/http://45.148.120.23:91/vmtools.exe/

Hash values

74cbde4d4b4ac4cae943831035bff90814fa54fd21c3a6a6ec16e7e3fb235f87
1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9
ba8a7af30e02bd45e3570de20777ab7c1eec4797919bfcd39dde681eb69b9faf
24137ac3dcad6a12abd58611a5d0c8b9
ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f
4c44efc7d9f4cd71c43c6596c62b91740eb84b7eb9b8cf22c7034b75b5f432d9
30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6
606d786a265ae7102255027b044432cf
d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c
90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0
1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce
9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739
f3e8f2ef4ad949a0ada037f52f4c0e6000d111a4ac813e64138f0ded865e6e31
5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581
af26d07754c8d4d1cb88195f7dc53e2e4ebee382c5b84fc54a81ba1cee4d0889
6e5d840ddeedc3b691e11a286acd7b6c087a91af27c00044dd1d951da5893068
c93d2c2d8d9b51a6c1b778c7ddd40455
245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa
c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5
90a92f3c19f15879335e846a601b9d6820b8f1a9
a983350925f47c7e50d2ddbe0fec695f
6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50
8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2
c8a8fed939a230f28be44547366433c734d7836e
525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9
e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3
a49ee90ee45bcb717b1e65facf8f8ce3
f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b
8bbd277a2f5f2981ce222e0dd7590c165af2b8fc
43761c642fe3e53ea841953a2a6e277a704f51c3
87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8
092479f5e1a584e89b8e03ccace849bd
b19ccfa8bc75ce4cf29eb52d4afe79fe7c3819ac08b68bd87b35225a762112ba
5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970
de500875266fd18c76959839e8c6b075e4408dcbc0b620f7544f28978b852c1c
667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c
da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9
23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae
b6a63b6250dcebdcb112729cc2311a80
52c95947a748f7fe660d4e67ec33e8cf6a4a70e8
7ea706d8da9d68e1214e30c6373713da3585df8a337bc64fcc154fc5363f5f1f
bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec
dcadcac4c57df4e31dd7094ae96657f54b22c87233e8277a2c40ba56eafcf548

Domains

/d3ktcnc1w6pd1f.cloudfront.net/

IP Address

/3.0.93.185/

/172.245.92.207/

Reference Links

Grayling: Previously unseen threat actor targets multiple organizations in Taiwan - Cyber Security Review (cybersecurity-review.com)