Hive Pro

Threat Level

Amber

THREAT ADVISORY

ACTOR REPORT

Kimsuky targets South Korean entities with phishing campaign

Date of Publication

August 26, 2022

Admiralty code

A1

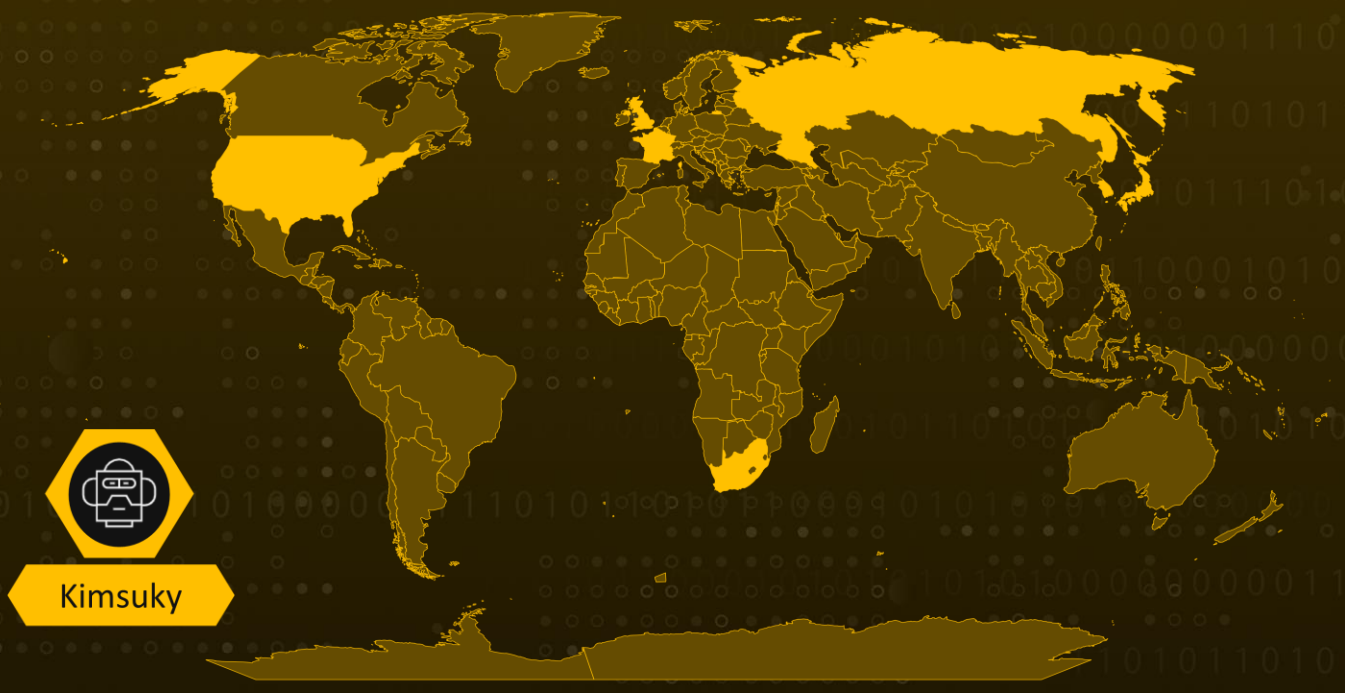
TA Number

TA2022185

Summary

As of 2010, Kimsuky has targeted the governments, think tanks, media, and education entities of the United States and South Korea. Early in 2022, a new attack cluster GoldDragon was observed targeting media and a South Korean think-tank. As part of its new cluster, the actor sends spear-phishing emails with macro-embedded Word documents.

Actor Map



Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**TA0002** Execution
T1059 Command and Scripting Interpreter	**T1059.005** Visual Basic	**T1204** User Execution	**T1204.002** Malicious File
TA0011 Command and Control	**T1105** Ingress Tool Transfer	**TA0005** Defense Evasion	**T1140** Deobfuscate/Decode Files or Information
T1218 System Binary Proxy Execution	**TA0011** Command and Control	**T1104** Multi-Stage Channels	**TA0006** Credential Access
TA0009 Collection	**T1056** Input Capture		

Technical Details

#1 Initial infection occurs when Kimsuky sends its potential victim a phishing email. As soon as the victim clicks on the link, the actor establishes a C2 connection and delivers a malicious document embedded with VBA. As soon as the fetched document is opened, a connection is established with the second C2 server.

#2 Finally, Windows executable-type malware is delivered and is used to steal information from the victim, such as file lists, keystrokes, and stored login credentials from web browsers.

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONs	TARGET INDUSTRIES
Kimsuky (Velvet Chollima, Thallium, Cerium, Black Banshee, ITG16, TA406)	North Korea	Information theft and espionage	France, Japan, Russia, South Africa, South Korea, United Kingdom, United States	Cryptocurrency, Defense, Education, Energy, Government, Healthcare, Media NGO, Pharmaceuticals, Policy Institute

Indicator of Compromise (IOC)

TYPE	VALUE
Domain	attach.42web[.]io attachment.a0001[.]net bigfile[.]totalh[.]net clouds[.]rf[.]gd global[.]onedriver[.]epizy[.]com global.web1337[.]net

TYPE	VALUE
MD5	238e6952a990fd3f6b75569feceb26a2 edde6a385c86f60342831f24c3651925 b6ba7e07b4867e4bd36dc9713744aedc 7a3e966d30fe5d52cfe97d998e8c49cb 596251e844abdaa77eeca905f0cb7677 3fa45dcacf2193759086319c0d264341 75ae786fe89491dc57509801c212fa8b c0097cfa2e05ab1d18cf3dad93d98050 b80d15cbb729e6ca86e3b41924407c30 85f24b0f10b77b033e6e66ae8b7d55fc 40de99fb06e52e3364f2cd70f100ff71 5f38c57f83ee5d682ddf692442204fba b237b484c5c0fb020952e99b1134a527 96f5ef3d58a750a6db60f2e0566dc6e6 3265b2d5e61971c43a076347fb405c4b d9f2acfed7ede76f110334e2c572b74e c4a69dab3f8369d2f823c538590de345 23b5811baa6cc9e562185571579ce5bc 62b0fa29bcc317c59c5f5e7fd3a867bc 8bb7c8e8b723b02ffdcf6ff52444a810 8d28e28c1ee6f133441b6d71f7f8bcba 32dda97cab8876215d771e398dd10f84 226f7677052f636a9a4f6e95b9e8b864 2c73cf2356a9005850fb2d07d024b2f2 f37afe7e072b26a2de22e16074f62294 bd0f789ace4def9196ce26588c3f41f8 a889a22d09286d71fb83fae5c0ff1c96 a87614a2c7c66c7f13f0b170e4837ede 3361fa242eb7e6162fd4682471f4e952 b18d2d4e77fc567306d406c75b75dc53 ea5c59741ff0ac27f45c4a9a508514c2 86b523d2f19e1628e8c74602a51ebff9 0a050b4239032ec76f1e244bceb435eb 07b2457f6e71d0b75693b6fecf9c88e7 e5682b7fb53cb478550df7f51bca6175 4433edb19f368e56d903a4ed0aa25a2e 72016ca15de6a0528fb9a9d0ac85d8b5 8b6d472fa9ec0023d7a35bdd7b8b2d4f 611c1a2771108730fde487bbb6d680d4 bb6662ed3f058a737674be6749c7e6f2 407fd3c14a19a6b682b0b7ecca0b0c8a 157e31eb70e2f28059f100f85317fcce 7cb5dca82ad330db0dde62a34ad3f692 7953f5b1ed7b0b0ac778a2d47f44195c c41f178a41aec6e7a28723ea70c3bd3b

TYPE	VALUE
MD5	e4df8b86d669e1eb36add172972bcb27 20389c0e7f03e5df407ffcf5811eee09 e36cee3e23f3ab5557e547ce02b5bf3d ddf966990bc4bdb40b67b8eda0ae1fd7 beb6601397e208d2793aaa7be297b0f4 c791d7fc5216d4035825f4efb714ba0e 71def16f01ce0f57afe7b19c104a24e5 a871511ef8abae9f103a3dfe77b12b6d c5ad15506ab05f054d547587111d6393 25eed4e06f9ed309331aaa6418ebd90d 809f60589ee8be7daf075446c2180eaa 5b5247ee7b43f51092ab07a1d1a31936 8735788b2422c7ab910953178af57376 490b2496434e6a20dae758d0b6fc6e00 56b5fec59e118ba324ccee8a336f7f12 56df55ef50e9b9c891437c7148a0764a 8289771e7eeffd28fb8a9e1bdeb3e86c dfb8d00ce89172bfc7ee7b73b37129a9 7fb868e6baf93a86d7a6a17ac00f4827
URLs	hxxp://koreajjjjj[.]atwebpages[.]com/1[.]hta hxxp://koreajjjjj[.]sportsontheweb[.]net/k[.]php hxxp://kpsa20201[.]getenjoyment[.]net/d[.]php hxxp://o61666ch[.]getenjoyment[.]net/post[.]php hxxp://o61666ch[.]getenjoyment[.]net/report[.]php?filename= hxxp://yulsohnyonsei[.]atwebpages[.]com/1[.]hwp hxxp://yulsohnyonsei[.]atwewbpages[.]com/d[.]php hxxp://yulsohnyonsei[.]medianewsonline[.]com/1[.]hwp hxxp://yulsohnyonsei[.]medianewsonline[.]com/1[.]txt hxxp://yulsohnyonsei[.]medianewsonline[.]com/info[.]php?ki87ujhy= hxxp://yulsohnyonsei[.]medianewsonline[.]com/ksskdh/d[.]php hxxp://yulsohnyonsei[.]medianewsonline[.]com/post[.]php hxxp://chunyg21[.]sportsontheweb[.]net/s[.]php hxxp://faust22[.]mypressonline[.]com/1[.]txt hxxp://faust22[.]mypressonline[.]com/info[.]php hxxp://hochdlincheon[.]mypressonline[.]com/f[.]txt hxxp://hochuliasdfasfdncheon[.]mypressonline[.]com/report[.]php?filename= hxxp://hochulidncheon[.]mypressonline[.]com/c[.]txt hxxp://hochulidncheon[.]mypressonline[.]com/k[.]txt hxxp://hochulincddheon[.]mypressonline[.]com/post[.]php hxxp://hochulincheon[.]mypressonline[.]com/c[.]txt hxxp://hochulincheon[.]mypressonline[.]com/down[.]php hxxps://225b4d3c305f43e1a590[.]blogspot[.]com/2022/01/1[.]html hxxps://225b4d3c305f43e1a590[.]blogspot[.]com/2022/02/1[.]html

TYPE	VALUE
URLs	hxxps://3a8f846675194d779198[.]blogspot[.]com/2021/10/1[.]html hxxps://c52ac2f8ac0693d8790c[.]blogspot[.]com/2021/10/1[.]html hxxps://leejong-sejong[.]blogspot[.]com/2022/01/blog-post[.]html hxxp://dmengineer[.]co[.]kr/images/s_title16[.]gif hxxp://dmengineer[.]co[.]kr/images/s_title17[.]gif hxxp://dmengineer[.]co[.]kr/images/s_title18[.]gif hxxp://leehr36[.]mypressonline[.]com/h[.]php hxxp://leehr24[.]mywebcommunity[.]org/h[.]php hxxp://weworld59[.]myartsonline[.]com/h[.]php hxxp://weworld78[.]atwebpages[.]com/info[.]php?ki87ujhy= hxxp://weworld78[.]atwebpages[.]com/s[.]php hxxp://weworld78[.]atwebpages[.]com/hta[.]php hxxp://weworld79[.]mygamesonline[.]org/hta[.]php hxxp://glib-warnings[.]000webhostapp[.]com/info[.]php?ki87ujhy= hxxp://glib-warnings[.]000webhostapp[.]com/s[.]php hxxp://glib-warnings[.]000webhostapp[.]com/hta[.]php hxxp://0knw2300[.]mypressonline[.]com/d[.]php hxxp://21nari[.]getenjoyment[.]net/info[.]php?ki87ujhy= hxxp://21nari[.]mypressonline[.]com/s[.]php hxxp://21nari[.]scienceontheweb[.]net/r[.]php hxxp://chmguide[.]atwebpages[.]com/?key=cWFLQ2hCU3ZTaUNha3hVaGdZSXRyQT09 hxxp://chunyg21[.]sportsontheweb[.]net/info[.]php?ki87ujhy=

References

https://securelist.com/kimsukys-golddragon-cluster-and-its-c2-operations/107258/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

August 26, 2022 • 1:45 AM

More at www.hivepro.com