Mphasis
The Next Applied

North Korean Group Kimsuky Exploits DMARC and Web Beacons

Date: 24th April 2024 | Severity: High

Summary

Kimsuky is a state-sponsored, North Korean APT group (AKA Velvet Chollima, Thallium, Black Banshee) that has been active since at least 2012. The group mainly targets South Korean entities, such as think tanks, industry, nuclear power operators, and the Ministry of Unification, for cyberespionage purposes. It was also observed operating against organizations and individuals in the United States, Russia, Japan, and various European countries.

Attack Vectors

Kimsuky usually obtains initial access using spear phishing email messages, either with lures relevant to the attacked entity or with general lures, such as COVID-19 related themes. The messages contain malicious attachments, usually Microsoft Office documents (Word or Excel), with a Visual Basic macro code. Once the macro is enabled, various types of malware are deployed into the victim's system, such as BabyShark, AppleSeed, Gold Dragon, and FlowerPower. Other initial access methods utilized by the group include watering hole attacks and drive-by-download through torrent sharing websites or malicious browser extensions.

The Rapid7 Labs reported new targeted attacks by Kimsuky (attributed with moderate confidence) against entities based in South Korea. The threat actors sent their victims CHM attachments that contained BAT files and VBS scripts leading to the creation of scheduled tasks for persistence, which was followed by information gathering as Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies to spoof various personas, including think tanks and non-governmental organizations (NGOs). These fake personas are commonly used in Kimsuky's social engineering campaigns to increase the authenticity of its phishing messages leading the recipients to engage with the threat actors.

On April 16, 2024, Proofpoint reported that Kimsuky had been abusing different tactics, such as Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies to spoof various personas, including think tanks and non-governmental organizations (NGOs). These fake personas are commonly used in Kimsuky's social engineering campaigns to increase the authenticity of its phishing messages leading the recipients to engage with the threat actors.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domain	• regard[.]co[.]kr • well-story[.]co[.]kr • gbionet[.]com • myaccounts[.]gmail[.]kr-infos[.]com • mail[.]kumb[.]cf • gyzang0826[.]blogspot[.]com • rfanews[.]sslport[.]work • bizsonet[.]ayar[.]biz • cf-health[.]click • update[.]ssnuh[.]kro[.]kr • nid[.]naver[.]onektx[.]com • wilsoncentre[.]org • pollor[.]p-e[.]kr • default[.]tokyo • naver[.]koreagov[.]com • wilsoncenters[.]org
File Hash	• dddc57299857e6ecb2b80cbab2ae6f1978e89c4bfe664c7607129b0fc8db8b1f • b970be67522c225f159c6873b160bf3e74520c1df544dee833fbf16cb3c9d8fe • 934731692b12fd182acbc698dd3f8ef59984aa4e7ef56e124f9851852878817e • caa24c46089c8953b2a5465457a6c202ecfa83abbce7a9d3299ade52ec8382c2 • 4a1c43258fe0e3b75afc4e020b904910c94d9ba08fc1e3f3a99d188b56675211 • 0fa91cac5712cfc0848af092190fd3d09948f1a7750547f0f16d1867dac6288a • c3b0b1fa477f54168b44465894a4d04ddff95740c3c4c0e25ab4e11668865c6e • f0cbe4867b5c9d32cd2fb583458bc10453b38d680e965b0cce7012616c16c31a • f6000ad859571d0da5a32341303c0a39e33d31a6ebd5a64fb607c622196fd689 • cd82c4b157a7b819457eef2c1ac95e9c3b740a6977cc7c0cd89a5070f0ac3e3e • be5c7cc70281e9f5c613fa4ed5c65ce48ded74a49db6c74f5d0fb96c680a97d6 • 622cb6a772b0034f741aa58a50f1155a2a4240021c929d90fbed4182877fa579 • 453f27c7a32f292e9da197359067a2769d3bb537bd12d716e082f3a5622f3084 • f4e0f55d80915c86d7de4c88368856eef71a8219c473de87427e3168cd612a7e • a7a987fb55f4c1921ea7f6c8f2acd3817bacbee2fdf30c0e4f50ee23656e0b51 • 8433f648789bcc97684b5ec112ee9948f4667087c615ff19a45216b8a3c27539 • 7b77112ac7cbb7193bcd891ce48ab2acff35e4f8d523980dff834cb42eaffafa • 18ee06625f7bddadafa8c256d63a123f4e69d5488f88828052fd7803b3aa8b3b • c62677543eeb50e0def44fc75009a7748cdbedd0a3ccf62f50d7f219f6a5aa05 • 2060d58311e927aec8f2e8803f5bf5f8072e0a8cf85adf0c1a667d9221a394d2 • 4a4224f6c898ead010964627a9dcee369eb6205afc52a23253eb1eb7349b020a • f39d8455cc4b611c9f85b42becbe8409aae450aad784e64e08b4d77565cdd469 • b4fbad52624e6d1e0b9e5899c5279bd9a8653aee24f252dc29a0cb40b36b2db5 • bc3e41e97d9bba05ed033b14ac2c26796cedb32fde88ee88367a627641c09dfa • 97e5c0876d91e78cf7e30ae898ce9b0fb5f250c6
IP	• 104[.]168[.]145[.]83 • 45[.]114[.]129[.]138 • 38[.]110[.]1[.]69 • 162[.]0[.]209[.]27 • 104[.]128[.]239[.]70 • 159[.]100[.]6[.]137 • 107[.]148[.]71[.]88 • 45[.]77[.]71[.]50 • 5[.]61[.]59[.]53 • 23[.]106[.]122[.]16 • 104[.]225[.]129[.]103 • 146[.]185[.]26[.]150 • 104[.]225[.]129[.]86 • 209[.]95[.]60[.]92 • 175[.]45[.]176[.]27 • 216[.]189[.]159[.]197 • 141[.]95[.]84[.]40 • 45[.]76[.]93[.]204 • 152[.]89[.]247[.]57 • 172[.]93[.]201[.]248 • 23[.]236[.]181[.]108 • 209[.]127[.]37[.]40 • 91[.]202[.]5[.]80 • 192[.]236[.]154[.]125

URL	• http://spmode[.]smt[.]docomo[.]ne[.]jp-ssl[.]work • https://3a8f846675194d779198[.]blogspot[.]com/2021/10/1[.]html • https://myaccounts[.]grnail-signin[.]ga/v2 • http://myaccounts[.]posadadesantiago[.]com/test/Update[.]php?wShell=201 • http://login[.]microsoftonline[.]org-view[.]work • http://leehr24[.]mywebcommunity[.]org/h[.]php • http://navernnail[.]com/fkwneovjubske4gv/android/facebook[.]html • http://heritage2020[.]cafe24[.]com/plugin/kcpcert/bin/list[.]php?query=1 • http://login[.]ssltop[.]work • http://comment[.]poulsen[.]work • http://eastsea[.]or[.]kr/?m=e&p1=00000009&p2=b&p3=b0f8c73c7c1d4093d502ed6d3c491a16eb86375c • https://rfa[.]ink/bio/ca[.]php?na=start1[.]gif • http://heyondparallel[.]sslport[.]work/ • https://rfa[.]ink/bio/ca[.]php?na=secur32[.]gif • https://sankei[.]sslport[.]work/ • https://login[.]daum[.]kcrct[.]ml • http://help[.]octo-manage[.]net// • https://mitmail[.]tech/gorgon/ca[.]php?na=dot_eset[.]gif • http://nidlogin[.]naver[.]com[.]ec • http://www[.]bignaver[.]com • https://worldinfocontact[.]club/111/bill/cow[.]php?op=1drop[.]bat • https://www[.]webmain[.]work • http://myaccount[.]google[.]nkaac[.]net/signin • http://xeoskin[.]co[.]kr/wp/wp-includes/SimplePie/Net/suf[.]hta

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.proofpoint.com/us/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-information-gathering
- https://www.infosecurity-magazine.com/news/kimsuky-exploits-dmarc-web-beacons/
- https://thehackernews.com/2024/04/microsoft-warns-north-korean-hackers.html