Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

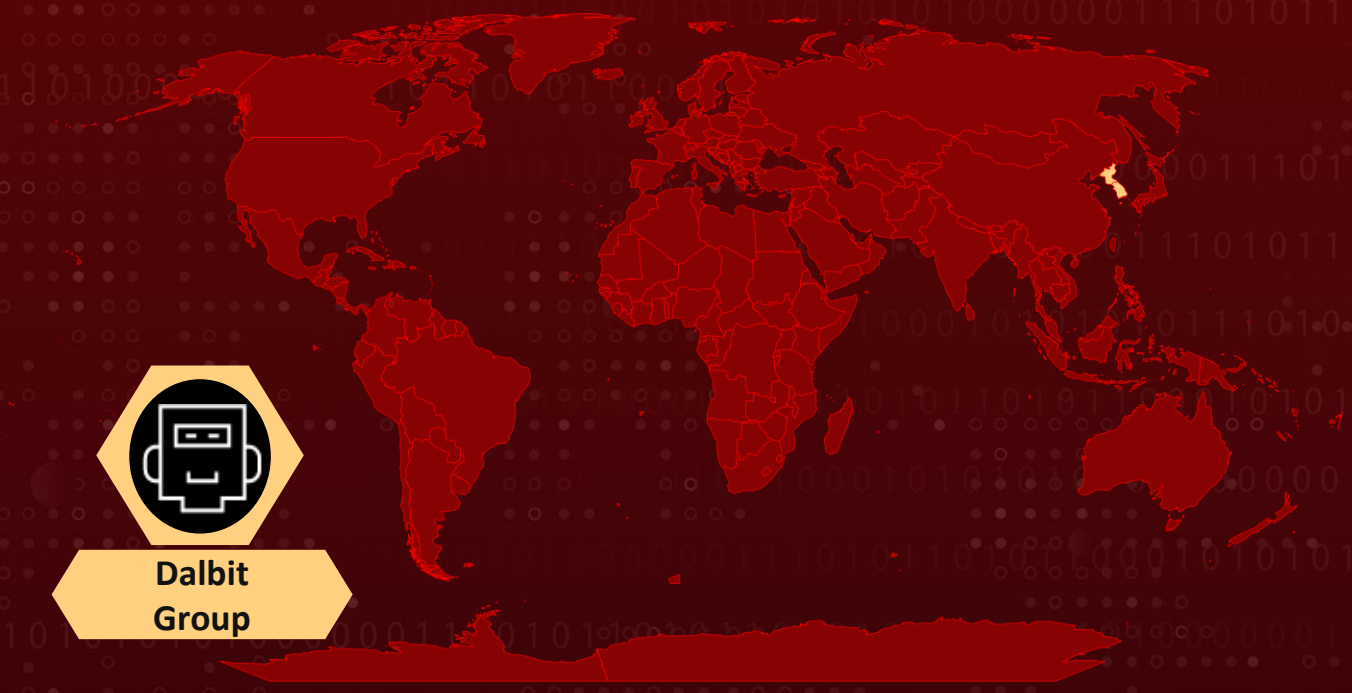
Dalbit Threat Actor Launches APT Attack Campaign Against Multiple Korean Organizations

Date of Publication	Admiralty code	TA Number
February 16, 2023	A1	TA2023085

Summary

First Appearance: 2022
Actor Name: Dalbit (m00nlight)
Target Countries: Korea
Target Sectors: Technology, Industrial, Chemical, Construction, Automobile, Semiconductor, Education, Wholesale, Media, Food, Shipping, Hospitality, Energy, Shipbuilding, Consulting

Actor Map



Actor Details

#1 Dalbit is a threat actor group that has been active since at least 2022. They have been targeting Korean companies, with more than 50 confirmed attack attempts so far. The group relies on open-source tools and has lacked any distinct characteristics to profile them.

#2 They have been using a hosting server called "m00nlight.top" as their C2 and download server, which is how the ASEC team decided to call this group Dalbit (m00nlight.top) after the Korean word for 'Moonlight'. The group typically targets mid to small companies, but some major companies have also been affected.

#3 They are known for leaving some infected companies as proxies and downloading servers to later use them to communicate with the threat actor upon infiltration of another company. The team has confirmed that 30% of the infected companies were using a certain Korean groupware solution.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Dalbit (m00nlight)	Unknown **MOTIVE** Information theft	Korea	Technology, Industrial, Chemical, Construction, Automobile, Semiconductor, Education, Wholesale, Media, Food, Shipping, Hospitality, Energy, Shipbuilding, Consulting

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actor through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0007 Discovery	TA0008 Lateral Movement
TA0011 Command and Control	TA0003 Persistence	TA0005 Defense Evasion	TA0040 Impact
TA0004 Privilege Escalation	TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration
T1059 Command and Scripting Interpreter	T1047 Windows Management Instrumentation	T1569 System Service	T1053 Scheduled Task/Job
T1136 Create Account	T1505 Server Software Component	T1098 Account Manipulation	T1134 Access Token Manipulation
T1068 Exploitation for Privilege Escalationbtain Capabilities	T1003 OS Credential Dumping	T1018 Remote System Discovery	T1046 Network Service Discovery
T1562 Impair Defenses	T1070 Indicator Removal	T1021 Remote Services(	T1570 Lateral Tool Transfer
T1114 Email Collection	T1090 Proxy	T1486 Data Encrypted for Impact	T1608.001 Stage Capabilities: Upload Malware

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	0359a857a22c8e93bc43caea07d07e23 85a6e4448f4e5be1aa135861a2c35d35 4fc81fd5ac488b677a4c0ce5c272ffe3 c0452b18695644134a1e38af0e974172 6b4c7ea91d5696369dd0a848586f0b28 96b23ff19a945fad77dd4dd6d166faaa 88bef25e4958d0a198a2cc0d921e4384 c908340bf152b96dc0f270eb6d39437f 2c3de1cefe5cd2a5315a9c9970277bd7 e5b626c4b172065005d04205b026e446 27ec6fb6739c4886b3c9e21b6b9041b6 612585fa3ada349a02bc97d4c60de784 21c7b2e6e0fb603c5fdd33781ac84b8f c44457653b2c69933e04734fe31ff699 e31b7d841b1865e11eab056e70416f1a 69c7d9025fa3841c4cd69db1353179cf fca13226da57b33f95bf3faad1004ee0 af002abd289296572d8afadfca809294 e981219f6ba673e977c5c1771f86b189 f978d05f1ebeb5df334f395d58a7e108 e3af60f483774014c43a7617c44d05e7 c802dd3d8732d9834c5a558e9d39ed37 07191f554ed5d9025bc85ee1bf51f975 61a687b0bea0ef97224c7bd2df118b87 9fe61c9538f2df492dff1aab0f90579f ab9091f25a5ad44bef898588764f1990 87e5c9f3127f29465ae04b9160756c62 ab9091f25a5ad44bef898588764f1990 4bafbdca775375283a90f47952e182d9 0311ee1452a19b97e626d24751375652 acacf51ceef8943f0ee40fc181b6f1fa 3cbea05bf7a1affb821e379b1966d89c 10f4a1df9c3f1388f9c74eb4cdf24e7c b5bdf2de230722e1fe63d88d8f628ebc Edb685194f2fcd6a92f6e909dee7a237 e9bd5ed33a573bd5d9c4e071567808e5 fbae6c3769ed4ae4eccaff76af7e7dfe 937435bbcbc3670430bb762c56c7b329 fd0f73dd80d15626602c08b90529d9fd 29274ca90e6dcf5ae4762739fcbadf01 784becfb944dec42cccf75c8cf2b97e3 7307c6900952d4ef385231179c0a05e4

TYPE	VALUE
MD5	bcfca13c801608a82a0924f787a19e1d 75fe1b6536e94aaee132c8d022e14f85 d6cb8b66f7a9f3b26b4a98acb2f9d0c5 323a36c23e61c6b37f28abfd5b7e5dfe 7b40aa57e1c61ecd6db2a1c18e08b0af 3665d512be2e9d31fc931912d5c6900e 1aca4310315d79e70168f15930cc3308 5e0845a9f08c1cfc7966824758b6953a 9b0e4652a0317e6e4da66f29a74b5ad7 d8d36f17b50c8a37c2201fbb0672200a b998a39b31ad9b409d68dcb74ac6d97d d5054ed83e63f911be46b3ff8af82267 e7b7bf4c2ed49575bedabdce2385c8d5 f01a9a2d1e31332ed36c1a4d2839f412 d4d8c9be9a4a6499d254e845c6835f5f 4eb5eb52061cc8cf06e28e7eb20cd055 0cc22fd05a3e771b09b584db0a161363 8de8dfcb99621b21bf66a3ef2fcd8138 df8f2dc27cbbd10d944210b19f97dafd 2866f3c8dfd5698e7c58d166a5857e1e cbee2fd458ff686a4cd2dde42306bba1 3dc8b64b498220612a43d36049f055ab 31c4a3f16baa5e0437fdd4603987b812 b33a27bfbe7677df4a465dfa9795ff4a 7d9c233b8c9e3f0ea290d2b84593c842 c4f18576fd1177ba1ef54e884cb7a79d 5d33609af27ea092f80aff1af6ddf98d 622f060fce624bdca9a427c3edec1663 1f2432ec77b750aa3e3f72c866584dc3 d331602d190c0963ec83e46f5a5cd54a 21d268341884c4fc62b5af7a3b433d90 6a20945ae9f7c9e1a28015e40758bb4f a29f39713ce6a92e642d14374e7203f0 7ce988f1b593e96206a1ef57eb1bec8a fc9abba1f212db8eeac7734056b81a6e 9f55b31c66a01953c17eea6ace66f636 33129e959221bf9d5211710747fddabe 48b99c2f0441f5a4794afb4f89610e48 28e026b9550e4eb37435013425abfa38 2ceabffe2d40714e5535212d46d78119 c72750485db39d0c04469cd6b100a595 68403cc3a6fcbeb9e5e9f7263d04c02f 52ff6e3e942ac8ee012dcde89e7a1116 d82481e9bc50d9d9aeb9d56072bf3cfe

TYPE	VALUE
MD5	22381941763862631070e043d4dd0dc2 6b5bccf615bf634b0e55a86a9c24c902 942d949a28b2921fb980e2d659e6ef75 059d98dcb83be037cd9829d31c096dab cca50cdd843aa824e5eef5f05e74f4a5 f6f0d44aa5e3d83bb1ac777c9cea7060 0ca345bc074fa2ef7a2797b875b6cd4d f6da8dc4e1226aa2d0dabc32acd06915 0bbfaea19c8d1444ae282ff5911a527b a69d3580921ec8adce64c9b38ac3653a c4e39c1fc0e1b165319fa533a9795c44 fb6bf74c6c1f2482e914816d6e97ce09 678dbe60e15d913fb363c8722bde313d e0f4afe374d75608d604fbf108eac64f a03b57cc0103316e974bbb0f159f78f6 46f366e3ee36c05ab5a7a319319f7c72 7bd775395b821e158a6961c573e6fd43 b434df66d0dd15c2f5e5b2975f2cfbe2 c17cfe533f8ce24f0e41bd7e14a35e5e 011cedd9932207ee5539895e2a1ed60a bc744a4bf1c158dba37276bf7db50d85 23c0500a69b71d5942585bb87559fe83 53271b2ab6c327a68e78a7c0bf9f4044 c87ac56d434195c527d3358e12e2b2e0
IPV4	205[.]185[.]122[.]95 91[.]217[.]139[.]117 45[.]93[.]31[.]75:7777 45[.]93[.]28[.]103:8080 103[.]118[.]42[.]208 101[.]43[.]121[.]50 45[.]93[.]31[.]75
URLs	hxxp://sk1[.]m00nlight[.]top:80 hxxps://fk[.]m00nlight[.]top:443 hxxps://aa[.]zxcss[.]com:443

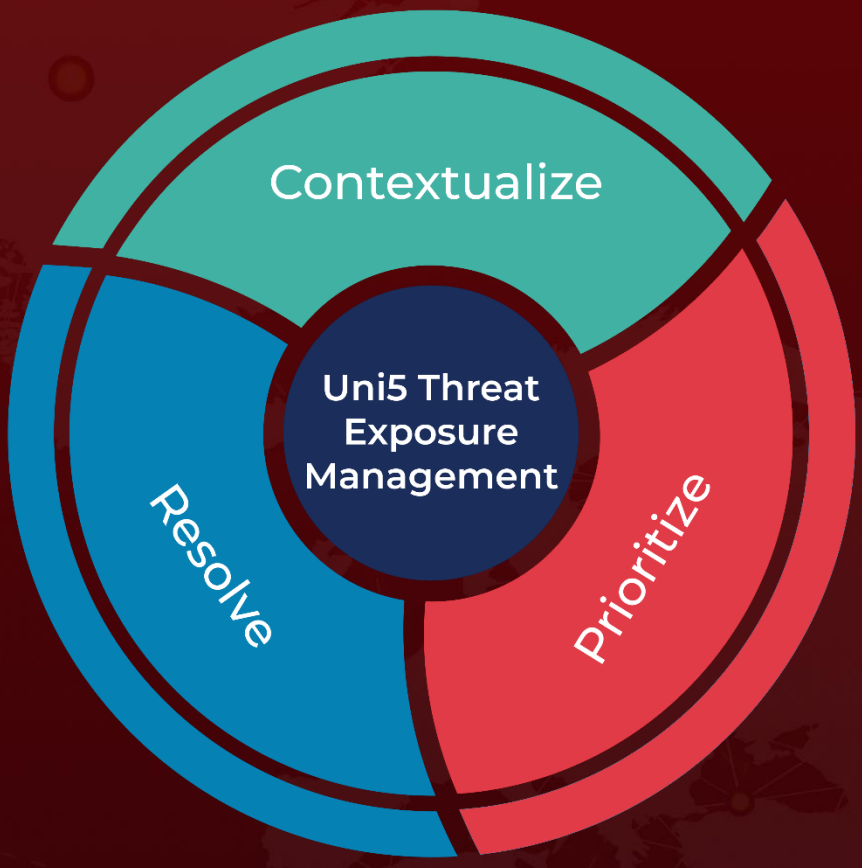
References

https://asec.ahnlab.com/en/47455/

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

February 16, 2023 . 3:00 AM

More at www.hivepro.com