Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

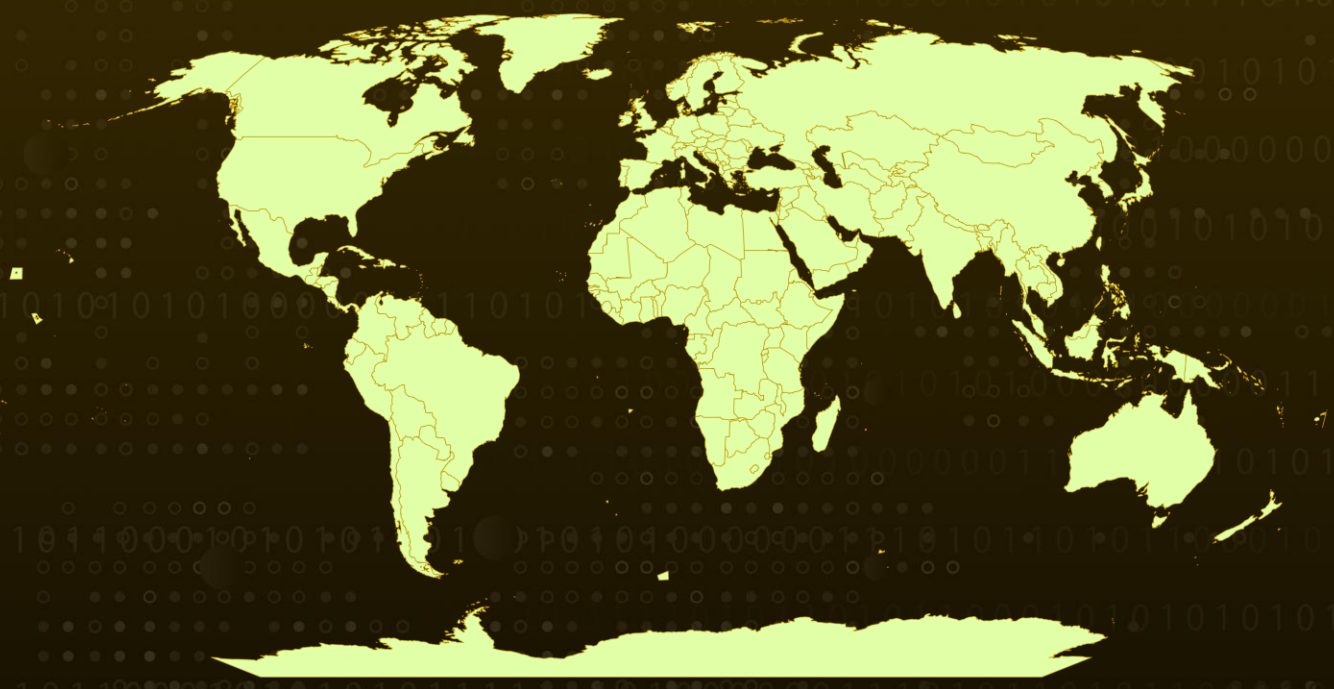
Novel Smishing Kit Leverages Cloud Platform

Date of Publication	Admiralty Code	TA Number
February 19, 2024	A1	TA2024063

Summary

Attack Discovered: February 2024
Attack Region: Worldwide
Malware: SNS Sender
Attack: SNS Sender, a malicious Python script that leverages AWS SNS for mass SMS spamming, presents a novel approach to cloud-based attack tools, particularly in the area of smishing. The ARDUINO_DAS threat actor is linked to the operation that uses this cloud capability to send out a lot of smishing messages. These messages contain malicious URLs that aim to steal the personally identifiable information (PII) and payment card details of the recipients.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 SNS Sender is a unique tool that leverages AWS SNS for large-scale SMS spamming, introducing a novel approach to cloud-based attack tools, particularly in the field of smishing. The script's creator, known as ARDUINO_DAS, is a well-known figure in the phishing kit community, and there are established links between this actor and other phishing kits designed to harvest payment card details and personally identifiable information (PII) from victims.

#2 Scammers impersonate USPS, notifying users of missed package deliveries, likely testing cloud services for mass SMS phishing texts. The SNS Sender Python script operates by taking a text file containing AWS access keys, secrets, region details, phone numbers, sender IDs, and message content as input, along with a list of phishing URLs named links.txt. The script configures the AWS boto3 client to send SMS messages.

#3 The script necessitates AWS credentials, which can be sourced via different attack methods, including phishing, credential stuffing, or exploiting vulnerabilities in the AWS infrastructure. During execution, the script iterates through the list of AWS credentials and regions using a while loop, replacing each occurrence of the string "links" with a URL from the provided links list.

#4 Over 150 phishing kits are linked to same script developer, many with a USPS theme. Resources from these kits resemble those in previous Smishing campaigns. Attackers may utilise this novel method as a first line of attack to spread their malicious payloads. This script, which is now concentrating on PII and payment card information theft, could eventually spread malware, including mobile device spywares.

#5 SNS Sender is a technique with limitations, as it necessitates access to a suitably configured AWS SNS tenant. Since AWS typically doesn't enable SMS notifications via SNS by default, the tenant must be removed from the SNS sandbox environment. Organizations can enhance their security posture by thoroughly reviewing SNS documentation and establishing robust best practices.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0005 Defense Evasion	TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration
T1059 Command and Scripting Interpreter	T1059.006 Python	T1566 Phishing	T1566.002 Spearphishing Link
T1598 Phishing for Information	T1555 Credentials from Password Stores	T1036 Masquerading	T1586 Compromise Accounts
T1078 Valid Accounts	T1078.004 Cloud Accounts	T1204 User Execution	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	8fd501d7af71afee3e692a6880284616522d709e, 01b82c779de9ef59ecd814d6131433f7b17d7eb0, 03329461d8003aece83db2c124b5c2769dd0300e, 03b0cc3f1576d0d719f5ac5dbba582a9c10e64e0, 040e07a1c4cbc7eb9fb2a8ecfb865c0a2f4db5b9, 04676e36b9e11f32fd675e96dd721a5a215a0641, 0544db064ecb8fd8f36e96ef31d031447011c711, 0547074a7cb42a67a933d70c302b626f4e10a86e, 09ddd1b6f3dc1323ad86d458da05f5be605c8e7a, 0a8ab120e03ed49e18ce3246b9d00f547fd9432c, 0bb8a3a478d1143a04fb8abd8aa9c116282cc700, 0eaa126cf4414684763b415aabc08e262ee7c194, 0fb6fa2855a39f7010d3a1bcc0c08e739747785c, 1024d7c1a10e94d0f926cff649a9bd9a0c5df6ba, 103a49c6c4f71ab5bbcaa01df89aef80e0c90229, 106b42a1a6401f6ff3cb38f66d0668ac22fbc59c, 10fe02acfa1053210387bc312f1ff9529eaeba35, 138a00f5e6ef81560cdfe25f2ab087c24e839efd, 14ea8aa63539498773bb0d4bea5fbede05f1c17d, 17a2515096e6afe5976f57887c89d3efe285ed06, 1a97f72dedbdf13b13baa4c535398af25a78a28e, 1b1940f128bb4f3420ebc4b5ab1a7b165e70003b, 1d0a54f030e8b68bbf1256811fbb4a284ce31fda, 1e85b4cf222387cddc0f2977d5c9f4a5eb03db06, 1fa655639ee1f7d9c8e3157346f65d351d4b3450, 1fb3a8a17123f82bf39ae93ede40273f155d5fa1, 1fe0823655c30cabf51816ed1048f647172d29c8, 20813f948849a05f84ed1b6a707ffc6965d17c1e, 25dd30bda5bbfa7af884c0d3a71857b6abcb8222, 27b6aaa536200b085d611af07b0c05df8a856eb8, 29a4771a04afce2b789fe34b42a12d2fa65073ab, 29d49c1d21c9e97c757db81db594e55b15587f98, 2ac1467e567bc6e950b8aee96d898b71f9cf5849, 2c62c5f3e4166be99bf985a0c5f08cfe5795221d, 2d4f45cdfe0793431e0134376b309f1707a4e2e6, 2e9bb5c725eee402a36d64f63e07f72451eaec03, 319569a20fdaf2fa356f6e33e575a5a613da79b2, 32a21398869e2e221552da49fe1d4beba11ad2ca, 342d6e453f6a02c43ca4dee045f89cbdaa97926c, 357df6a8740bca2b81b62a3a429b2fef5cc883a8, 38fcec4299789a1ba16099df0842aa196c34dde6, 3b15bf62091a80ec32a2c3af92da5115641cf13b,

TYPE	VALUE
MD5	3ba42572bd49882280306fc72759016c1ea90e7c, 3c6dfef72f703bd8a2779a40cef39c4eb2305e69, 3d920ba992668bbb303a6680251c54c928fec988, 3f31c8c8bf2acdbb3cbe792b2728b3a2eadccaec, 3fc724ee8958f941168e16e06ed8f0eccffacde7, 403ed75a0a86783a39e65aac0ca8d69d43f7a562, 40840c0b6bd9a6a25dd864e7812cb1ee499b10bf, 45a39f3af4ca67dea1f920a7bd03fe43b4b38bec, 492a0031807ea7defcfb6a0be058580adac88345, 4aa1f81a313c991532379f68808a59fdbecef2de, 4c95a04759f5edc679122c013d2bb2570cef78dc, 4cdbc5d865172d4026a624f0aa56959875ba562c, 4d8bcefef73e03784fd104b8cec8bb2e3b47c89b, 4f636146bc6661795a4fbde68c5ca5b48e4a462d, 508d218b811aaea176b51f577a2cb74ff59ddf6e, 50e6703a85b4e72834cef4438f29777c0e73af54, 533ba3e5bacf6c982cc827b6aef62817897cf8ea, 53c26c8f577e45ba188e18b89da4b54ff41970d0, 563bc88fd217b1af0301e7eec2b03051a7236054, 56d51c8d5959d33ba4c52643a6436380e4f9fd8b, 589a185002c75260b66a29a21939a751d1b49585, 5a61394c2b1b0da534a348ecd714810a57194574, 5a6f197b77317d5d80dbe59984ccffa11cbc28ac, 5aae678fdaada1e58e88fe9a8eabfddfc1fafed1, 5bc0e77c722c8b973e8d2627002da3503e26dbde, 5dc5dc2206059359df9bc5056dca634b8ca13004, 5fe779032a8edf0866832903aac4caa4c22d65cc, 60077d66f395c7af28537338bd8fed0e5f108617, 601c2e36a2f284ef3bb4752b364da53afe480537, 60d209585249f32d0ad24ca295911729d8f56496, 64a8d7093ed1f3737901110118c768fb9ded4882, 64cb6b72523df13628d2f43f400c719a556c5d86, 658a6fe9f5700426d2a6b85dc035ba54b847eede, 6594a9357d39e377032fc2b5094ee2f68248bffe, 687f843a50e75ea74b8c51487356ee2b1ebfe359, 6911cb39a03184324406f79042b648b8ed89c2d9, 6c1eefaba836d8a4f86ab8cc7d9a514f045827bb, 6cd850c489930ef8d2438174ab38d4c33bc70c45, 6d0e9ce56f99c87d9d70e0522b96c625783aece2, 7935a5760e10976d9eff013735c303069c669e72, 797acd73e43b3f56961d0c687d86009fec832aee, 79f93db9c9b5f42c7b26b79c926eb3dfeaee3571, 7c53c7119bf6be6c5b149a1fdcb2c22b39bc1470, 7c6d96174246fe907a1cb7fbe0f2592c1f8b48b7, 7edcdc353071b1c44ce4a8ac33670378a86eb1ba, 83e8e7da62463b79970442d2b0de2eccf36450f7,

TYPE	VALUE
MD5	847bb302b6107ac93a669c09552ca158a1440596, 87091170ae9ec6e0641d1e689a22e11324e2e4c6, 87093850d8084a9a1b1881e0959acf41fcf8799c, 87b41c7f499be3b765628874b37d2d0f84d53517, 88dfbd8036b122a1efa32b222f985447c7c80b41, 8952fbe59931daba401f615bf06b90547b6171a7, 8ac6dd99742dd328b690fb6f0552f2c4df2566c6, 8bc41965baba7f5e25d4bbb0519c1e4c573734c5, 8f06a9204f9a354cdf4dbf4c3ae870d5a386de59, 9004df92c9a9427767fdca02b9a1378cff42dbce, 91065e8ab12e9fce202c0eac0290cb1bd6c46ae2, 912a376b255e3b873a73767679e0fbe9a1b01446, 91562cad5eb7a9568190fa4b84da4de50ed3d274, 95197a29d05d2043771bc97a5ded6086f6dfbbd2, 95e707b5f9257913a36fb276d25e7312a9b86156, 97fba04a848da3c09bd906b6b3adb4aa9031e471, 98b85e3e2bcff8b5032ddbb9758174dec2bacf58, 9954725c56a9060c90b8d5cd0483fc6808f39bd1, 99d35595f41a9be3fc077d37599447c096ce66cf, 9a2ac6259c2707b34546bee8b5a4eec677716299, 9c4593c93cc5a5d7712bee10574823ebca9f6674, 9f2faa971f0f4fd783e34d11cba67b261b54cc5c, 9f9fbf77fd4c3aeb1542589efdc45d4e328da56c, a19ac9df01a0bc64e636054b0a728e024ade61e9, a2163de2f5056d64a27e96a73f7858b79d47ad06, a38087ce0515cd30fb3580ba12840bc610429649, a7ec178adabbb8eb533a81c658ecce56a9e697da, ab9baecfdf85033e65d59652e666b7328cb0960d, abddb05ed3b75cae4354044bad05e5662cbfbab5, ad0d4cfcc7c35a9a96ad071a4863dbe8f83d87db, adf4765cb74c708496fa39c8c002e32b6f0c1e71, aebdd69f0bbbb8d0d3c231f0fbe1516edc5e0216, b212145149ca3f1c62e991bcf31357ecc8b17851, b2192b99736376f9e5705e81d3b55bce408e17a8, b26d632d14e91634ba01df0b3b18907657025563, b5d8b89c88f32e2c0a9166f48e87f853a497b667, b66c21bb8ef8ffa3143f3a6bae2c67f14eef069a, b6e3c52c1bd309f596b4ba50d0f7487b66bd5701, b7420fb4774e755bdb3062d12eb750687c115a3a, b7a6780990590ac3ebb632b9198b63531d645129, b841b4ae0629a5336356bce88794e0744f72f98b, ba5d94f8852f5cdee14e2bf8e1f0eb1cf599ecfb, bc0e3f1c5b323daf31ecff178c620be0c03efb64, bc3ebc37a77acef15b827e4ee43aeb839bc5605d, be0ca87b74a345d62814cad3916133e3e655acc6, bf9c85e3ed9a3f0a51eeda6284be24b507a5770f,

TYPE	VALUE
MD5	c117393f640ccd1d5fa5b002fcc3803498b61a2d, c283818259bceaddfd62554fdf37493d413b9b84, c547caad7d7517b2026e3c17461c249a925460d3, c60830bac782f58c61a81821da8153f639c86a74, c92c68b12ba817df7eb83666bd478466cb1c423a, cabbe92c9b5acb779f9fb76b1f8e3ed77a44935d, cb27a59e95c5d1b81219ba1cae4225f7340b16f2, cc4306140f14bcec70f103f4213e96e24d065381, ce701e5c639158563455c28bc39efd2051196932, cea7151a8260b9e48b687d40a9062ad361efed2d, cf4872e3e9f580b1865f68bae6b31bca0f0e22e6, cf7f11b4a39792531118058bd1c8ba2a2cabc486, d71c9f3d3aba149d13d7434731423c164cf2f002, d77c1f97339ba891286c10f6456a1e7f44b3c3bb, d78275c82d2f10ba5ed6bfbfec37686a7646d8ea, dc7fd807e8c9fc10185dcc47bc14f7460a4228b3, dd682090d3815b52cf74b22280d1b8db02ef339e, df66269b6826273650716524219dd83cf0302dc4, df7ee28ca069f798489cb4dc2ff1295bb6377a6f, dff37819d805c0fa99f11a466f583f2f752af8b0, e2498ab48872162bab97e7a5737376cec2a5b401, e7dc9e8f82cab9de0ec3b92693cdca726c5d72a6, e95528bd91158bab9d1e998969951209f6d8a3b6, ea4c4495ac7d68543cb423d34704e8fbfd595f6b, eab2f2b4a924397d22ecd1a6e8758de585e9fdcc, ee7105ca1065b6f0f6ce4b041b1a0a95b5678790, eefcbc6b32fdf7167db0b9a455b3c8c0f8d4b58d, ef5a5d04dc048a3c1f6a415be1ad74e1478b802e, ef8b8d215b4cc107495b3957fbedd2317f642cd9, f01c586c97d68847d1f373f7fd45444af26aff7a, f28b3d223a0c351f70ec0c7680e80083c232a470, f351bd5595b1eb2196f5c2ef1c519a7a8a7967dc, f35fd34a90c7a9b827c1d9417b8f088e8302ba01, f3b5e4840139ab0465b3c432d19bae1365e923af, f5b1256e407fb37d44a54ba29dc6fd4815cfde55, f754e4a59c49c0b3e653fdd8fdc04078810524dd, fae99902bef8011459926e4a69b85ae2cf0c0914, Fc9d7c59645450be5887f938aaacbca2b0b3f1f9
URLs	hxxps[:]//perwebsolutions[.]com/js/, hxxps[:]//usps[.]mytrackingh[.]top, hxxps[:]//u-sipsl[.]cc

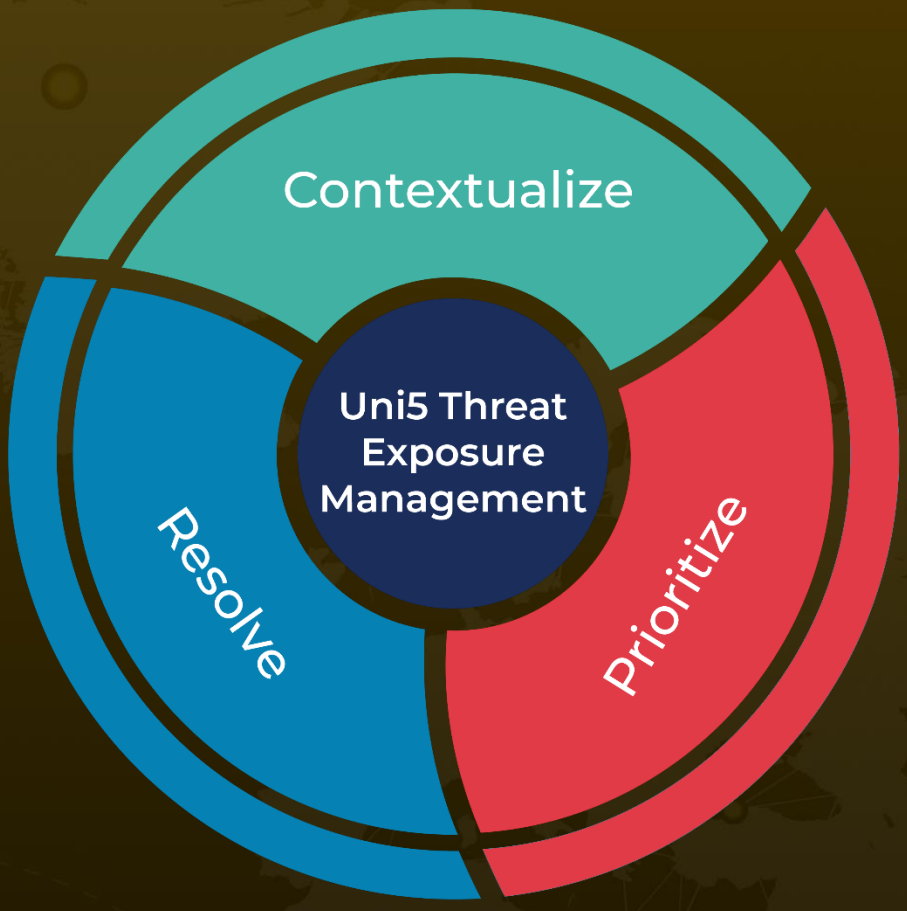
References

https://www.sentinelone.com/labs/sns-sender-active-campaigns-unleash-messaging-spam-through-the-cloud/

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 19, 2024 • 5:20 AM

© 2024 All Rights are Reserved by Hive Pro®

More at www.hivepro.com