Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

AllaKore RAT's Grip Tightens on Mexican Financial Institutions

Date of Publication	Admiralty Code	TA Number
January 29, 2024	A1	TA2024035

Summary

First Observed: 2015
Malware: AllaKore RAT
Targeted Industries: Retail, Agriculture, Public Sector, Manufacturing, Transportation, Financial Institutions, Commercial Services, Capital Goods, Cryptocurrency, and Banking
Attack Region: Mexico
Attack: A threat actor has been targeting Mexican banks and cryptocurrency trading since at least 2021. Using custom installers, the actor distributes a modified version of the AllaKore RAT, an open-source remote access tool. The campaign cleverly mimics the Mexican Social Security Institute (IMSS) in its lures, embedding links in seemingly legitimate documents during the initial stage.

Attack Regions

Attack Details

#1 A financially motivated threat actor is currently directing its efforts towards Mexican banks and cryptocurrency trading entities through the utilization of tailor-made installers, delivering a modified iteration of the AllaKore RAT—an open-source remote access tool. This activity has been conclusively linked to an unidentified, financially motivated threat actor based in Latin America. The campaign has been operational since at least 2021.

#2 The lures employed in this campaign leverage the naming schemas of the Mexican Social Security Institute (IMSS) and incorporate links to authentic, innocuous documents during the initial stage. The samples exhibit a more intricate installation structure, deploying the .NET downloader compressed within an MSI file, a Microsoft software installer.

#3 The downloader meticulously verifies the target's location in Mexico through network IP location services before initiating the download of the customized AllaKore RAT. Notably, the observed adversaries targeting seem particularly interested in large companies, many of which boast gross revenues exceeding $100 million USD.

#4 AllaKore RAT, a straightforward open-source remote access tool scripted in Delphi, first surfaced in 2015. It was most recently employed by the threat group known as SideCopy in May 2023. The payload of AllaKore RAT undergoes significant modification, enabling threat actors to transmit pilfered banking credentials and unique authentication data to a command-and-control (C2) server, primarily for financial fraud purposes.

#5 The threat actor has augmented the RAT with new functionalities, specifically tailored for banking fraud. This includes targeting Mexican banks and crypto trading platforms, initiating a reverse shell, extracting clipboard contents, and fetching as well as executing additional payloads.

Recommendations

Enhance Email Security Protocols: Strengthen email security measures to filter out phishing emails. Educate employees on recognizing and reporting suspicious emails, especially those with disguised LNK files or compressed attachments.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect any suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1189** Drive-by Compromise
T1204.001 Malicious Link	**T1059.001** PowerShell	**T1218.007** Msiexec	**T1480** Execution Guardrails
T1070.004 File Deletion	**T1140** Deobfuscate/Decode Files or Information	**T1105** Ingress Tool Transfer	**T1071.001** Web Protocols
T1219 Remote Access Software	**T1056.001** Keylogging	**T1113** Screen Capture	**T1041** Exfiltration Over C2 Channel
T1204 User Execution	**T1059** Command and Scripting Interpreter	**T1218** System Binary Proxy Execution	**T1070** Indicator Removal
T1071 Application Layer Protocol	**T1056** Input Capture	**T1204.002** Malicious File	**T1036** Masquerading

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	ADV.exe, App.exe, chancla.exe
IPv4	192.119.99[.]234, 192.119.99[.]235, 192.119.99[.]236, 192.119.99[.]237, 192.119.99[.]238, 23.236.143[.]214, 23.254.138[.]211, 23.254.202[.]85

TYPE	VALUE
Domains	flapawer[.]com, chaucheneguer[.]com, hhplaytom[.]com, zulabra[.]com, uperrunplay[.]com, uplayground[.]online, praminon[.]com/519, trapajina[.]com/516, zaguamo[.]com/500, pemnias[.]com/433, isepome[.]com/435, narujiapo[.]com/435, manguniop[.]com/422, debirpa[.]com, dulcebuelos[.]com, iomsape[.]com, bstelam[.[com/431, rudiopw[.]com/430, ppmunchi[.]com, pelicanomwp[.]com/422, andripawl[.]com
SHA256	94489764825f620e777a34161d0ce506a49eec20bc27c3d63370e493a737d50e, 884789b63fe432938e1bb76c9976976c1905b74c2974340a60eb7ea8261d48fb, b18e0c7c9569b33187e2beaf3318e99b50ed40c54e7dee8a26ce711bc782b150, 4085c9829e2b18fd4721688dc25c0611f260b6e4f827b667999d9603cfe5e2d7, 66f5b7ca8760fb017b0750441707c24eaa916d5b8aa021b3aa92082c6129ca22, 0a3aa8c2485a3b8525f044f33c6d268ab79e1942885792d95f6a1c0c45be6106, 84a468a25a8c65dac51f520732d2e9e6afa6b59e4b2f485c262a9bd305cd61c0, 9402128b9602fbb485be887def8cd72c3265cd09f6dbf4e0a3ad2ea42da66870, e4a6be2fb70603f1545641240680b44e21b5601e8016c0d144711423eef9778e, d5ac0f4efa8396ae9ba74cc3ea2a62485e4d49a930efed0d69b043162bb66cc2, d63447877be48156032cc9ec9def7e25d62e7bc544bd3e19da75c0f55e09dcc0,

TYPE	VALUE
SHA256	7bb22d7013dede7b866ab25cbe32246228c46bd8a951b5a72557b7280ebb066f, 2867d87bbc088b8cc50ff66f1d9c064cba978433cdb900649bbbb44370f8cbd1, b00fee1c275d12a05ca8a06ab54ffac2e3e8da68fd2be450f34c36c8a38e4887, e7e2a6fe7325ad7945a6020202ab5581e0a204f8b8ad9ffc48c18f129a6f8c46, 42f1d24e135b9d3e4fd38e1ec3ab20cae495ec3526ae4037d937c6344914e923, 88a9e666d4231a98a909ae5780778b85ffdb8a5207b8f7dfca2a0911cc0f6580, 872c58b72962c1f0696b26563425c6734cc2246d1ea3375f675c1bd1ca915e59, 49de6df83c5fe55c4e45b5744203513832f0435dbbd7913a3ce7f827afe51236, 0eb20898a0a3c1f4a4210a819fa0bd8f8574db3413db8b85e381ab0c1963791a, d928ce7383d8582163c36773d1d97360a5ded812d11ee0faf99c7afa78251850, 8a1381a829776220ec4bf0a9d36cf6842a5638b0190e667ee696bab04b8e7c9f, 0835d21b60e3443892988d675f20393d79503ca6e37a889d9f7da19c321b3426, 4276b4b4504edff275a4d56b99f66b23c48b49f4081abab36bf4d8f88818e2da, 8cc14643ec452aa35e709ae34b874e0f070a20b174e7eeb2a046351a329cdde9, 0eeb357abcd3864538dc26000f3a1d706c2c330fadfb845f7fc350b382d00c4e, 61037a3321e143d85cdf77abf31f33ca5a701da0b84cef172bcf89457dfb4e7d, 0324d8ed29829e5fa7add2bab1e73f2ad0094e80867caf57d35369a5e22fe79c, 2444dd2bb0a0fa0631935ddeb829b753d1ba46c9149ee45f79794903f26e16fa, 19d357351a29f6530624556bd31c475d56ea9ad76f31eb28f7d251fa3c751d62, da0b73d2f42f0232762f7c8d3eaa6863969f1982b798cd9fc19431c901ae4635, 2843582fe32e015479717da8bf27f0919b246a39495c6d6e00ac7eca8b1d789c, b1489b216fb25bcf57329546c160800645c0a6620add3c8323e2b589d7150e9e, a72018420f8aab9cb431d120bfa06acd09d777a88aa186ec495dffdc22395f0e,

TYPE	VALUE
SHA256	2a0d1c7354b43acd6fd0303beb6277db92691f03e37baea0c39249ae0d8b5301, 906d49817970955847f64d2f868e418579549e9cfa91c575f38342a1bd66ad4b, e01b10fc4131b8eec32148e559b95fd82da817166b831ae32a0fa89be883e8e9, 08f0954be207eaa1a85cdc9eed4ad2737613bbbf240a7c30b658b583c3ddef0c, 3499e5bd9daad587e05337bae5e953f279ebee20d9cf6d2a1707be28ce6295bf, 1230b1a189b17a4da79bc10bde0fbb439c37997c8f927d4a80c61b006d8b3267, 17213aa5a43fcf6a6baf5e784f33411cd0fa3a2fb00418486085c5a24695af7c, c86f9d739ea3c6b57fd070892be9d1d4b3c50fca8a8c3e05cf84875378fcc649, b61c027adcef5d2108dc13735cef5d4bce295f13de6032f3fee5129be74816b6, 968f90a4567cdf67885c116379c792b4eeda1f7f8bd2cf34daf8c58b17f2ec0f, a65091e8912e4b65458041f866d37410b46e7a9432a57e0d7dc01ca4a21f3940, bf3e96bb6273890f48b566e9d484e0e747e8f21e3dbd6606a39edf98faedc7b1, 6d3a50a354bcf2df226ce1065563755b3ab16d2e440900e3b80a9f0571c0f73a, da61eb41bffd50a07793ccc8b2ead76f5c49313445f07aa685c28523bbf39a00, caa7ef0b9a6ea51752813b7107348f46a3475acf9b3f1242e675f6a1296ccb2c, eaf26e1d12e0ae355441499bdf9d13c582540f3876bddfdef95c676f185609b8, cee2730a6e4100e3b865cb6fee41f77ec5a8bfce186b1e121ebb4236cd3dff88, e1246fbac51f8369292aec96270dd4b2a62fd148d9b6f2ca8ee208631237a44f, f292911c11a15001ca66e90df341f8763d4d149482f06f85cc2873651d205a6b, 8d4d672eeba756c7ace20aea90219c8f7409b23ecc9c2eb47a31b1cd2d3577a6, 7474cd11f62a53f0f3035fb62753561067cd771ec3e5d73823e74d4f4b8d31cb, 74f637b21f7c68e6d56f0d64378336b28f500d82d4eb876d5b1cbbfe3a952ac2, bbd94254223f4ec3edbcc44c5d6d5ae5029c8d9c4512f02d3c61d2a28c3c5416,

TYPE	VALUE
SHA256	31e060d82ef68613d26b5e47c3934d482fc2975dad71fa6e677900cc8a938116, 55455d2488d127fc7bb6976821c36ad5661a5e57e2d57dcc7ae7cb12ba7282d3, 301f27dc88655927ce45b0c1138b4931b0d3aa7dcfdd424315d5c7339c540e52, 5c1306596589d0b0c0f0d04be6687e5c2dbe92fbba493760b0ded7a47942fbb1, bc81f08ad4c543a35f899da8d45787751b50d221d67dae083d62097631ace059, 582aa139fb1c315f68106cc2e50c10835874e8bc77aeb7302453f9aa3c25d920, 7bced78c519befdb1b7ef3b973250f4ee2d3c2404309cea372df16b8ff5b1d84, 8185e9784adfd6c2f1a286a724e7e374008667ae1f50cfa1a58451a5c33af536, 05d0dd9916646c6144506bb26cab500d807ab015609bd19634e890fbeb63e48f, f8262a0c746bbfbb3e7cb17398953cd8391cdf416b759d4be1f1fc11611f4eb3, 14f15b1d7951f078bbf412bb2ef774c812efff70280b86b8176994374c0e766d, ec1ea0b01ad6cd431c8441dc83537c3d9ef00994f9dd76a3041ff50c2526ce38, 53e196f293b4f99face97449d18106f7dc9df5b9170354d1c1da27f9ec71849c, a20672a07f3cf2e67682486c1a2b6684e9a50ca129260a74353d1664be25aa92, cdf35bb3a256d4bd4e09a2a9b19e4682a3952233c720e37d9ae88e4050b8473a, b9ea5ecbda6abd328bd7370d250fa9ab5a38a104955ac383cecee8ce581b9d80, 933858679466d57b4ea47003f08d864b1a417d7be75008e42ecd62f05dde7964, 3ad89c70d77b9fec35bbbac25d3dabca9d6c1fc055b8570a2d34b3af5ac58aef, 55f1b8346fc2e94791431a237d8a38fb6bb2014380b1905955d12bccb8c24e79, c1e18c6a611ccf23971a43fcdc0186d6a3f2bb0ee792140c35fc1e1a34582551, 225d10a0b3880eebafb327769e39a2484161e21e5d07ddef8fe16b65d2a90113, dcea0d579d3d6ab2d29a3665e3e0c3849ccd42abe390b80bf362c79088a1ebbe, 4865a260754a6a8740a85c40ef4185420334f9b21cc0d865295fdae4bb1e94a4,

TYPE	VALUE
SHA256	ae192d14a916ecdb55803830eace5ef820b1b520a751b6b689fa9591f6f292bc, bdc0a1ad95b1a62ae1e702681949fea485f42d5884aca78df02a64869688192e, c625ac5c134a74d84f8ce91504e41af15972ec71c064f7a5d31c588a8ff2c332, ea357305411b9c6b27657782e2bb14bc0c18149a7ad4093b30c12b041f785933, f76f5c12b81aa6d7fac0eeb4b775004c525ae50ebb049b6f4177417104eb8ef4, 2be8c01e5ffcabb566212268a63ef3c42db5c57d3e879abe99b06b48ac9bacda, 46f5ffcc04ea1eaf09cfce1a9329624c85a5c5435d91444a55ce02fceebfd2f7, ed7da8aef7dbe652b429d64a918a943c6586e1d4cec353c84663f8b451c09874, 3c1be333e85f0243cdbcecfd727e86d582569809e2c45fefb64261b473ca1734, f0dfa2297df28f64dc38da3a54bbef5c499691a8cf05de0f08e20f4f7077e67c, 40fc64907dcd0063e5f2b604fe78d0484d821cb9cda199d3cdca5e0219b43587, fc39aa0d2486c746f9b8d4d459a65517a21f961fb24ec25c4470f0b86e8c7cae, 4bfa7c32d9eb8f7468a1919dbf9698e971052c091de4b66b125ba18b04bbe607, d8e22f8b5964428b4a29e5aad9ec9186bd96e7d29bc56ede8821a24294629931, bc3fcaa746c261af6b72ee0720fa739d7f79df71709b7067f016e30578f94c22, 263bc3729f5785acb6647af950f3fe0a0cbbe05d2fcc9639276852ba39ecbaa2, f31a6b19572b668dbb473a0e43e53b9c1e5020b057421de8fc019c150ed3fb38, ee32169bef700d3dcceb86a101e188e5c0146a1104ee8809d1e031d93cdee36c, 9946fb2e81d07ad7780a20cf06b59bd27177c8bd6ed543e13089c47957adab1a, c5a4bf56670d51fed1e88050eddb003f39af0e22fbb01163679fef758b000392, 4524d47ca7b7d71764f12807fd3722e4b890388eb2f5bf975d58c6afd0221fb3, 8e2fc9de5da07a6cf6cfeb3349185e282cec5eed944cb66873136bd697389516,

TYPE	VALUE
SHA256	2f9f289224482204b0f3bb4f0af8fe99f235daea99fe435cbc53dcbb9bc22bb0, 434ec6d3575f72e680a8bf9211b3a853d80457644ff01d7acc41657b9bfdca24, eee76b24be7121434ec7ad1ca39792cbfec594916f8e143fad18698955ba0870, 81c5b7940a69854c72cb99d4af6a1092f0adc9182e9e8fd729b1857126d096ba, 13d88bcf312896fae6d03d59c564bc9521e0916096098cfe41508395955aab0e, 168ac972b7f0610f978e50b426e39938f889422b1bcfaf9cddf518e3e1ed9aa9, 2ff3cdb886b1caf3eaad9a2467bfa16b9269b88695b76bb6a0da481458e30aa3, 305cde85573131949fab5a3973525a886962c4f8c02558d3a215689a49f53406, 33578228c11ad0b3d86a198a32b602aa93a91d2feeae2fb2e83f8c6595c8acd9, 422c9471c29fe17457e142df1a567c273212019eb20b0b4783891c529c1248a8, 46c14c2f0d04710f53db16473877d3315c13e1a33a3236846a87e8f91808c8eb, 49a04f31e49cee3ae65e9d776bc0f8aedf40c52fafcd002ccf7de4044abec2dd, 52134d02cd77f8a65fd5b15c7c57ff2909ac39f0b5779592c533a18bf6b23879, 5961b42f8efad58c437bdad862a0337c6bcd57f7cbf35184f2de60f4609fd477, 673d4fe6f9e46fae37649c525f1d0d89cfd3b8310210dff4ddc7349418d9e80f, 6d516a96d6aa39dd9fc2d745ea39658c52ab56d62ef7a56276e2e050d916e19f, 89206ca169747d4aa70d49350415f21df7f1a00a3bf8d0c253b6beda2eb919d9, 8fce1d24cf952528169f473b9462724482511615ed31165710e5e3a74cefdd02, 911e45d053bdf3a41e812203ae29db739cf3505a4e37209936c1cc83ee42e8e9, 9221470c77b46bcd457951ae3a3d31d60ad4602ea9d152d51d1e4f9a5b3bca3a,

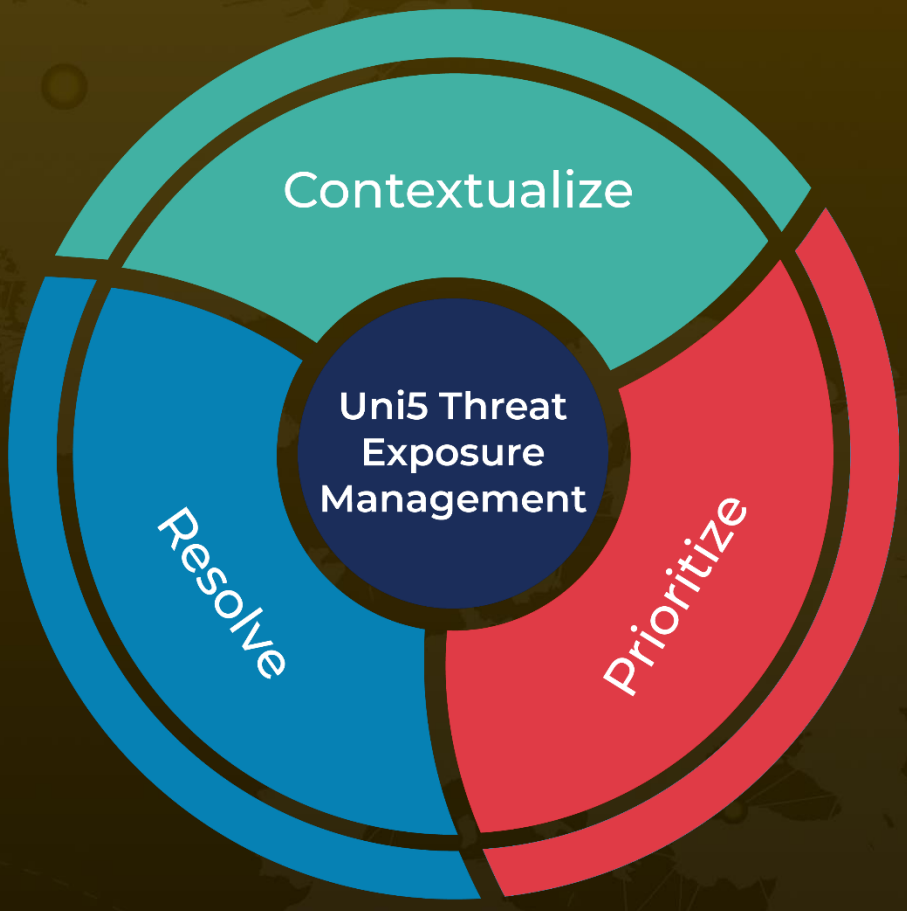
References

https://blogs.blackberry.com/en/2024/01/mexican-banks-and-cryptocurrency-platforms-targeted-with-allakore-rat

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

January 29, 2024 • 3:00 AM

More at www.hivepro.com