Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

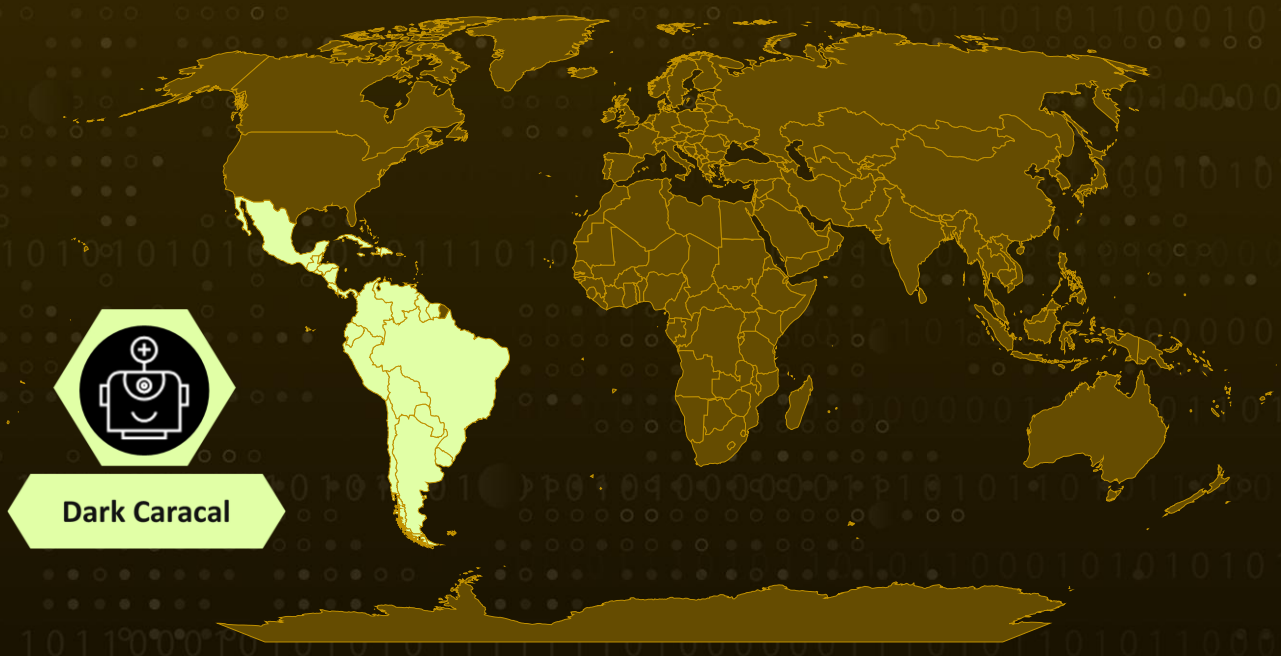
Poco RAT: Dark Caracal's Latest Cyber Espionage Weapon

Date of Publication	Admiralty Code	TA Number
March 7, 2025	A1	TA2025068

Summary

Attack Discovered: 2024
Targeted Countries: Latin America
Actor: Dark Caracal (aka ATK 27, TAG-CT3, G0070)
Malware: Poco RAT
Targeted Industries: Banking, Manufacturing and distribution, Healthcare and Pharmaceutical services, Logistics services, Marketplaces
Attack: Dark Caracal has introduced a new tool to its cyber-espionage playbook named Poco RAT. In a targeted campaign against corporate networks, attackers crafted phishing emails and malicious attachments in Spanish, signaling a clear focus on Spanish-speaking victims. Packed with a robust set of espionage capabilities, Poco RAT could exfiltrate files, capture screenshots, execute remote commands, and manipulate system processes giving attackers full control over compromised machines.

Attack Regions



Attack Details

#1 In early 2024, a new malware strain named Poco RAT was identified, named after its reliance on POCO libraries within its C++ codebase. A targeted campaign deploying Poco RAT was observed in 2024, focusing on infiltrating corporate networks. The attackers relied on phishing emails that impersonated financial communications. To evade antivirus detection, the attackers used blurred or low-quality images, tricking victims into opening the attachments. Once opened, the document redirected the victim to a malicious link, triggering the automatic download of a .rev archive from cloud storage platforms or file-sharing services.

#2 The malware was distributed through platforms such as Google Drive, Dropbox, and URL-shortening services like Bit.ly and Rebrandly. Each attack used a unique directory structure mimicking the targeted organization's name to enhance deception. Inside the archive, a dropper file disguised to match the decoy document's name was hidden, making it appear harmless. Upon execution, the dropper stealthily deployed Poco RAT without leaving obvious traces on disk, helping it evade detection. Additionally, the attackers modified executable metadata, inserting well-known company names to enhance credibility and bypass security scrutiny.

#3 Rather than running Poco RAT directly, the dropper injected the malware into legitimate Windows processes to blend in with normal system activity. Both Bandook and Poco RAT used dynamic API resolution to complicate analysis, intentionally triggering memory access violations to obscure execution flow. Each dropper instance also generated a unique encryption key based on a Ripemd-160 hash, making detection even more difficult. Once operational, Poco RAT granted attackers full remote access, allowing them to browse the file system, execute commands, launch applications, and capture screenshots

#4 Dark Caracal, a well-established cyber-mercenary group active since 2012, has a history of cyber-espionage campaigns targeting various industries. The group has continuously refined Bandook, adapting it over time to improve its stealth and capabilities. Infrastructure analysis of Poco RAT and Bandook campaigns revealed overlaps in their Autonomous Systems (AS), reinforcing the connection between the two malware families and their operators.

Recommendations

- **Enhance Email Security:** Implement robust email filtering to block phishing emails impersonating trusted entities. Use email authentication mechanisms like DMARC, SPF, and DKIM to prevent spoofed emails. Educate employees on identifying phishing attempts.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.
- **Access Controls & Privilege Management:** Apply the principle of least privilege (PoLP) to restrict user permissions and minimize the risk of executing malicious payloads. Enforce multi-factor authentication (MFA) to strengthen account security and prevent unauthorized access.
- **Secure Cloud Storage & File Sharing Policies:** Limit the use of external cloud storage services like Google Drive and Dropbox to prevent unauthorized data transfers. Ensure all downloaded files from cloud platforms are scanned for malware before being accessed.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1608 Stage Capabilities	T1608.001 Upload Malware	T1583 Acquire Infrastructure	T1583.003 Virtual Private Server
T1588 Obtain Capabilities	T1588.001 Malware	T1566 Phishing	T1566.001 Spearphishing Attachment
T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell

T1055 Process Injection	**T1027** Obfuscated Files or Information	**T1027.013** Encrypted/Encoded File	**T1027.002** Software Packing
T1113 Screen Capture	**T1082** System Information Discovery	**T1132** Data Encoding	**T1132.001** Standard Encoding
T1571 Non-Standard Port	**T1665** Hide Infrastructure	**T1036** Masquerading	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	94[.]131[.]119[.]126, 185[.]216[.]68[.]121, 193[.]233[.]203[.]63, 83[.]97[.]20[.]153, 45[.]67[.]34[.]219, 185[.]10[.]68[.]52, 77[.]91[.]100[.]237, 185[.]216[.]68[.]143, 194[.]48[.]248[.]72
MD5	a5073df86767ece0483da0316d66c15c, 2a0f523b9e52890105ec6fbccd207dcd, e0bf0aee954fd97457b28c9233253b0a, ec8746a1412d1bd1013dfe51de4b9fd1, fea98ca977d35828e294b7b9cc55fea9, c41645cba3de5c25276650a2013cd32b, 8778b9430947c46f68043666a71a2214, d8ec2df77a01064244f376322ba5aaf1, bbfbd1ece4f4aa43d0c68a32d92b17e5, 32c6c0d29593810f69d7c52047e49373, a2ea38d11bde2a4483b86321960d6319, e6f23ff5f55bcb05669732c6a519a75a, 27fabcf160575efc9ff6b7c93b35edd0, 8fe826ceee2242238f918e7bba5ba7e7, a12d326845a96a03867b2b70ca8f12ee, 40776099cf9098a626bae58763a503f6, abe2aa641f49f924a8c5bed6915b33a6, 18d4b1fb0a643fa86e815a3464c48f65, 5a21405b06a11ee03c24cc79ef910c3d, 812267e367c58c04d7c4800aa0f64603,

TYPE	VALUE
MD5	2ecada671f172d4142e66e40d6d70b1b, b179ead57646353b0460a578f206c9af, 5a4dd46d2eda27f97f88c2d4c5797114, 26e11dfbfc87bed3a47099b0d4131868, a4a846ef5641949f1d6033537c719ffc, f23043993fa2d4c4e4f04fb579c9745e, 8daa10aa4ff65bb5e274a79df6aae004, f5297dde39cda6b8423131af8f9220bd, 132a8a7c6a43ab61c6e9363f9c893905, 0c4f220e1c2fb895e0ca5cbdc17d202e
SHA1	d0661df945e8e36aa78472d4b60e181769a3f23b, f3a495225dc34cdeba579fb0152e4ccba2e0ad42, ce611811d9200613c1a1083e683faec5187a9280, f719b736ed6b3351d1846127afec8e0c68e54c1d, 63b4d283eaf367122ce0dec9fc0e586e63ef0c78, d8021edcb42b6472dded45f7a028aff6dfe5aaa6, da3ea31e96fba64fcd840e930a99e705eb60c89b, ce60069d5fdef4acced66e6fc049f351c465ee1e, 2ffdf164f6b8e2e403a86bd4d0f6260bf17fb154, 4bf76e731d655f67c9e78a616cf8b21002a53406, 5240860d0db91bd8e13a150676a3ab1917312c59, 6adc9cbcc5d3ce969d982f70728fd09ec3419a45, 1d1f21745a5ea01cc3387099caae111a3cb79e6b, 06813b2b554db0de2aa296d31f951fd0cccda7bb, 3b1264d2e156a09142847b6a18f70a3267c406e2, 43fc1530db54c356831f4fd96b81c1548c6b1a05, c02d9f23d6bf627b77e72cc55551aba15701945c, 8bddb48d29fb06b15a3314f2a1afc2839a22d5ce, 388371ea56bd79813ef53152220d7c64396528ea, dd75522dc6f64a9fa12723b8978cc682217056da, 2d30ce50578b95eed8feb093e0b8170a9d0b8994, 256fca02ae02ffa70e6ea54e6cb43b877486ee6b, 4982c139f6627c991c426827088baf25f345ab97, 617d867fcf5919a33c7b402ea85c6dbc03075fc3, 6fc2f4194e65dc8e4a29e71ca87ba3960df60fbe, 859c391e2181034eadc4d07ac1a58b73e358432d, b4c0700a6d325c439ca48c570c6736f6b3fce308, 11a892c4e2a67807ac161f9752a68f900dfb9b6a, baa2a99c0d53241324505d435908acf9506774d6, 605c4887f774e2f25d9601beea26ac383cd25293
SHA256	05bf7db7debfeb56702ef1b421a336d8431c3f7334187d2ccd6ba34816a3fd5a, 08552f588eafceb0fa3117c99a0059fd06882a36cc162a01575926736d4a80eb,

TYPE	VALUE
SHA256	0d6822c93cb78ad0d2ad34ba9057a6c9de8784f55caa6a8d8af77fed00f0da0a, 0fe11d78990590652f4d0f3afba5670e030b8ab714db9083fd0a981e0f1f48f3, 0ffc7ae741bb90c7f8e442d89b985def9969ebf293442f751ab2e69f4df226a8, 121d941ba5a6ff8d99558e0919f49b926fbcd00e3007aad14ac85e799d55473c, 12e849ffba407d5db756879fd257c4b736eb4b6adac6320d2f1916d6a923fa46, 13306775fdf506b706693deccb44ec364fe04dbf3c471227c2439c2462e19080, 1786f16a50a4255df8aa32f2e21f2829b4f8aaba2ced3e4a7670846205b3ac70, 18ba3612b1f0dbd23f8ab39b2d096bab0ed3438b37932f473c787e24e57e8397, 01e8536751080ea135c3ad7ae9187d06cdcccddfc89bc0d41ea4281eeb3e9fb4, 032ff087debc175342e01a3bb205fbd7ab2e724babcb24cc4b66f1d8df783612, 158255fa4a257953edf84323b4d7fef129ab55450919a66d6ce8bc9d78612230, 1e7d86f9ff5fd50aeeeb04040baad0ac0d84347d60e132458448096a758e9ace, 21ff46a6fc9173fcc147d7a5c603032c662c6c1f1b05c1bb1e30e20e168bb056, 247b0725fc0935131537dd00eb454269f3dd5c8c94002448c7b3c27a9aafc75c, 26ee4581ec0d064a1296e8178b016249977a483fccb89dd55ab6634aac4faa0f, 302c707321abc9eca4d14171a33c9c5207711d2a18acc81b31a40bb68d6bea99, 3c099ec7363407c9fb742beca81f97ecca93807e0f4c7fe73e019a3ccedbd220, 3cc284cecc3a8513d8ba664f88c1164312c049822f9deb009fd0f63dd0c22801, 918309457c875042e044510966083575a1635e977f1baed76b4f35815d631da1, 0864b87a18356bbe93b2e10f1deee5d4b705fc824899d227ced25c96390b8a0d, 57358c9f7f38a9364884cdcc4919ec3f7c71f147e4329d72867f29f1828aac4e, e5ce11d9bdc7433f713a6f7bd1c05b0a98355ad8a9995e0b5349b10c9d0df1b1,

TYPE	VALUE
SHA256	a6ac2fd5dc59f5300c930b3fd5ffd6ed6e4dc27a2707e0293d521c88de027d4b, 8a0beec469a4373a2ebb4b21f013c33e3d2c539514462df5ff88dc8df9e87b3b, c8d20ae481f17de8606b92ab3170daea423081bf854d4b6957d7f2dd114a1f6a, 289757c325556561c88a3918f3cc04251dc1d2fe2dbfc24acf8e635da7982853, e5bc162807af900cf73a3f9a3e4cc1c5b10f774f44baa3632f4af6465c80c464, D633aeb1600c3d02bd21df94ee70fdf78d722e21df8d4ff473d24f7c84ea5c5a

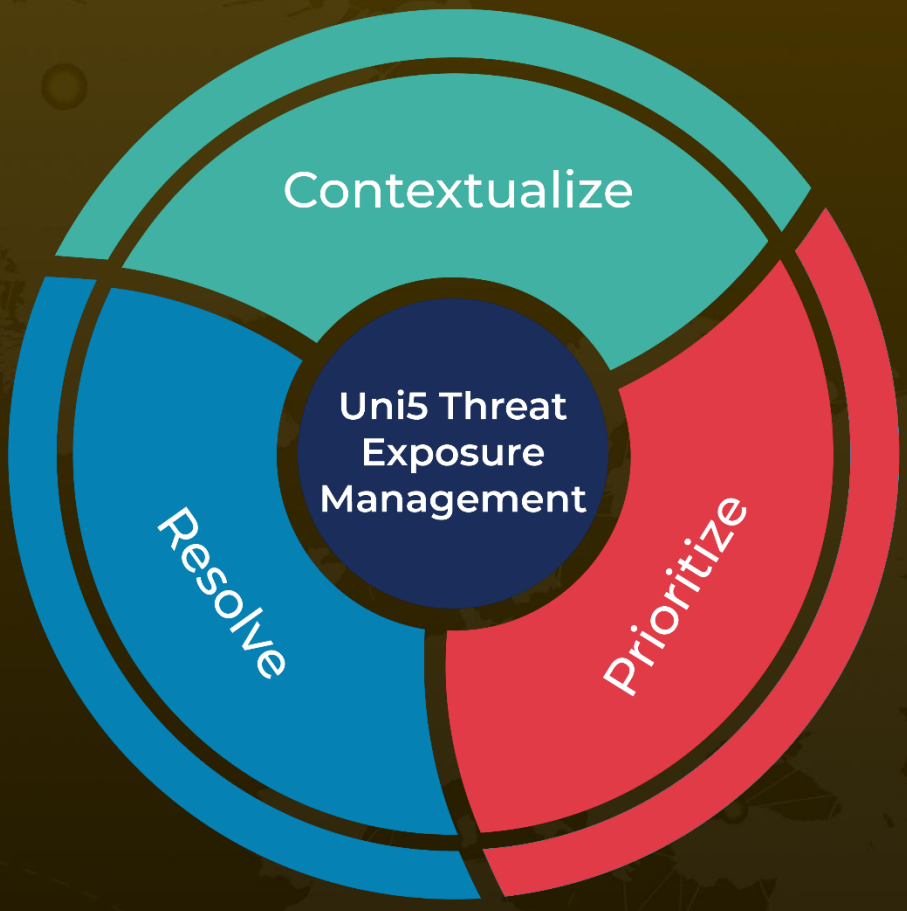
References

https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/the-evolution-of-dark-caracal-tools-analysis-of-a-campaign-featuring-poco-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

March 7, 2025 • 5:40 AM

More at www.hivepro.com