The evolution of Dark Caracal tools: analysis of a campaign featuring Poco RAT

By Positive Technologies

Published: 2025-02-28 · Archived: 2026-04-05 23:11:06 UTC

Detected attacks

Throughout 2024, PT ESC's cyber threat intelligence systems monitored a campaign deploying Poco RAT against corporate networks. The phishing emails and malicious attachments were written in Spanish, pointing to a clear focus on Spanish-speaking users. The attack chain is illustrated in the diagram below:

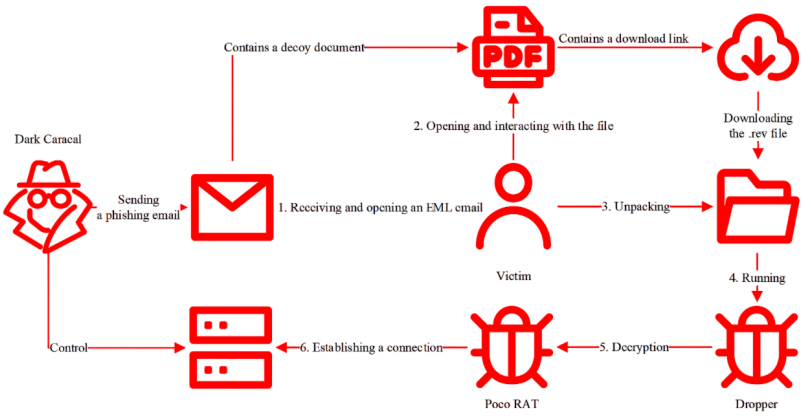

Figure 1. The Dark Caracal attack chain

The victim receives an email claiming an outstanding invoice requires payment.

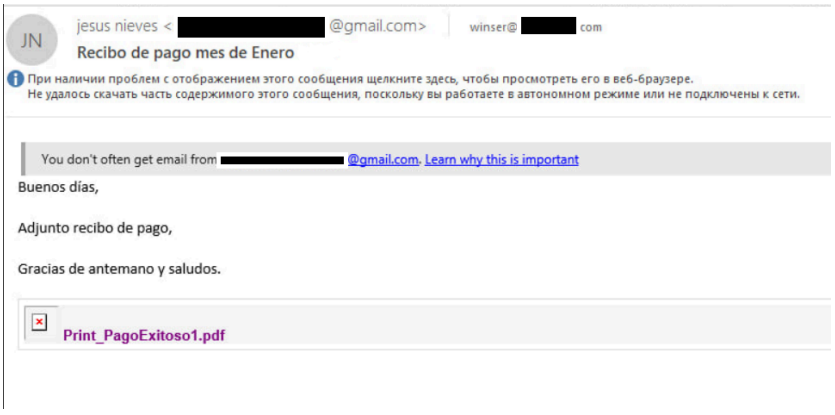

Figure 2. Phishing email with a PDF decoy

An analysis of the attached decoy documents identified the industries that attackers mimic to make their schemes more convincing.

The email attachment includes a decoy document, usually in PDF format, though HTML versions appear occasionally. It is designed to imitate documents from organizations in the targeted industries.

Tools such as Adobe Acrobat Pro DC and Canva are commonly used to create these files.

Metadata analysis has uncovered author and user names (PDF:Author), including "trabajo", Rene Perez, Keneddy Cedeño, and Mr. Pickles. Aside from "trabajo", which translates to "work" in Spanish, these names provide an easy way to identify decoy documents linked to the group.

```
'File:FileName': '92cdfc4d65bc496afa716b00bc34cb01f32529e58292338d762004d3f50b11fd'
'File:FilePermissions': 100666,
'File:FileSize': 41176,
'File:FileType': 'PDF',
'File:FileTypeExtension': 'PDF',
'File:MIMEType': 'application/pdf',
'PDF:Author': 'Mr Pickles',
'PDF:CreateDate': '2024:10:28 14:37:33+00:00',
'PDF:Creator': 'Canva',
'PDF:Keywords': ['DAGU3hMcwsQ', 'BAGUc81x0eY'],
'PDF:Language': 'en',
'PDF:Linearized': False,
'PDF:ModifyDate': '2024:10:28 14:37:33+00:00',
'PDF:PDFVersion': 1.4,
'PDF:PageCount': 1,
'PDF:Producer': 'Canva',
'PDF:TaggedPDF': True,
'PDF:Title': 'TRANSFERENCIA EXITOSA_0034.pdf',
```


Figure 4. Metadata of a decoy document

Decoy documents often slip past antivirus detection. Their filenames mimic financial transaction records between the victim and the impersonated organization. Blurred or low-quality visuals are common, possibly to lure less experienced users into opening them.
Once opened, the file redirects the victim to a link that triggers the automatic download of a .rev archive from legitimate file-sharing services or cloud storage platforms. This approach makes it harder to detect and block the malware's source.

Files with the .rev extension are generated using WinRAR and were originally designed to reconstruct missing or corrupted volumes in multi-part archives. Threat actors repurpose them as stealthy payload containers, helping malware evade security detection.

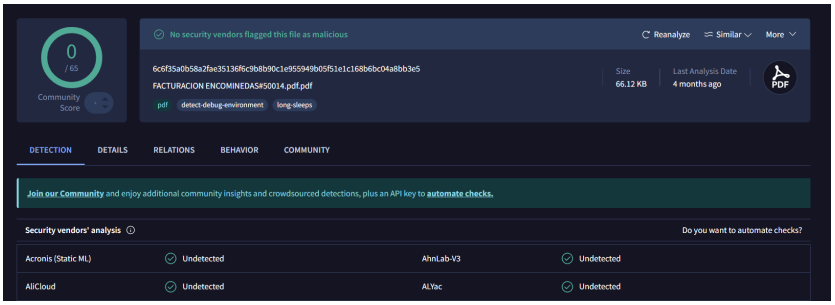

Figure 5. Antivirus scan of the PDF decoy

Table 1. Examples of decoy document names

File name	Translation
CONFIRMAR COMPROBANTE DE PAGO#00315.pdf	Verify payment document
FACTURA Global Supply Services, C.A.pdf	Invoice Global Supply Services, C.A
FACTURACION_DIGITALIZADA Industrias salineras c.a..pdf	Digitized invoice of Industrias Salineras, c.a.
RETENCION FALTANTE DE ABRIL solimsa.pdf	Missing deductions for April solimsa

Figure 6. Decoy document impersonating a file from the Venezuelan company Zoom

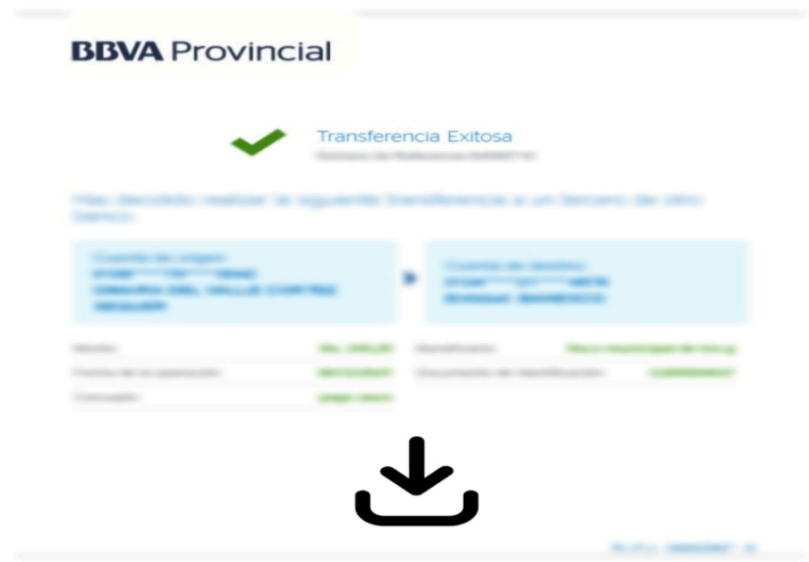

Figure 7. Decoy document impersonating a file from the Venezuelan bank BBVA Provincial

The threat group distributes malicious .rev archives using several methods:

- Cloud storage services such as Google Drive and Dropbox. Link-shortening services like bit.ly, is.gd, ja.cat, and Rebrandly are used to obfuscate URLs.
- CDN storage solutions. Each attack uses a unique directory named after the impersonated organization or related documents. For example, a .rev archive labeled NUEVAFACTURA might be hosted at farmabienoctubre2024.b-cdn.net.

Inside these .rev archives, the dropper file mirrors the name of the decoy document, making it appear more legitimate to the victim.

Poco RAT in action

Poco RAT is a backdoor designed to give attackers full control over an infected system. It allows them to navigate the file system, execute OS commands, launch executable files, and take screenshots. Every analyzed Poco RAT build has been packed with **UPX (Ultimate Packer for Executables),** shrinking the average file size from 24 MB to 13 MB. The size increase comes from its use of POCO, an open-source C++ library set built for network and internet applications.

The malware keeps an eye on itself by running a separate monitoring thread. Its activity falls into two distinct states:

- **Checking time** refers to monitoring how long the malware has been active, while collecting timestamps and assessing the system environment.
- **Disconnecting you now** is the state in which the connection with the victim's system is severed. This could indicate that the malware is shutting down or trying to avoid detection.

Once deployed, Poco RAT determines which **command and control (C2) server** to connect to. After establishing a link, the server regularly pings the malware with heartbeat messages to maintain persistence. Poco RAT then pulls system information using standard **WinAPI** functions, gathering:

- Username
- Computer name
- Windows OS version
- Free disk space
- Available physical memory (RAM)
- Current system time

Before reporting back to its C2 server, the malware checks if it's running in a virtualized environment. It looks for **VirtualBox** by scanning the registry path **SOFTWARE\Oracle\VirtualBox** and probes **port 0×5658,** a telltale sign of **VMware.** If nothing raises red flags, it sends all collected data to the server.

The gathered information is packed into a structured buffer, separated by the delimiter @&). An example format looks like this:

N35*@&)username*@&)pc_name*@&)win_ver*@&)free_disk_space*@&)ram*@&)time*@&)

The table below outlines the full set of commands that Poco RAT can execute.

Table 2. Command list

ID	Description
T-01	Send collected system data to the C2 server. This happens automatically when the malware starts.
T-02	Retrieve and transmit the active window title to the C2 server.
T-03	Download and execute an executable file on the compromised machine.
T-04	Download a file to the compromised machine without executing it.
T-05	Capture a screenshot and send it to the C2 server.
T-06	Execute a command in cmd.exe and send the output to the C2 server.

Poco RAT does not come with a built-in persistence mechanism. Once initial reconnaissance is complete, the server likely issues a command to establish persistence, or attackers may use Poco RAT as a stepping stone to deploy the primary payload.

Network infrastructure analysis

An investigation into the campaign's network infrastructure uncovered the C2 servers communicating with the malware samples. Scanning results showed no open ports, active services, or linked domain names.

Table 3. C2 server activity

IP Address	First File Detection Date	Last File Detection Date
94.131.119.126	24.01.2024	09.08.2024
185.216.68.121	16.09.2024	11.11.2024

IP Address	First File Detection Date	Last File Detection Date
193.233.203.63	13.11.2024	22.01.2025

Over the past year, analysis of malware samples interacting with these C2 servers has made it possible to track the threat group's movement from one server to the next.

Despite the absence of visible open ports, the malware establishes connections with C2 servers through specific ports:

- **94.131.119.126** — 6541, 6542, 6543
- **185.216.68.121** — 6212
- **193.233.203.63** — 6215, 6211

Who are Dark Caracal and what are they after

Dark Caracal has been in the cyber-mercenary business since 2012. It runs attacks for hire, going after government institutions, military organizations, activists, journalists, and commercial entities.

The group relies on Bandook, a remote access trojan that has seen multiple modifications over the years. It remains a flexible and effective tool for targeted operations. Unlike malware floating around underground forums, Bandook is off-limits to outsiders. Only Dark Caracal is known to use it.

A campaign linked to the group surfaced in 2023. It targeted Latin American countries, including Venezuela and the Dominican Republic. The operation followed a familiar pattern, continuing attacks that researchers had previously documented. In 2018, reports from EFF and Lookout exposed similar tactics.

Command-and-control server addresses linked to Dark Caracal are listed in the table below.

Table 4. Network infrastructure

IP Address	First File Detection Date	Last File Detection Date
83.97.20.153	17.02.2023	23.07.2023
45.67.34.219	26.09.2023	20.11.2023
185.10.68.52	05.07.2023	04.06.2024
77.91.100.237	03.11.2023	23.02.2024
185.216.68.143	06.02.2024	01.08.2024
194.48.248.72	19.07.2024	26.09.2024

The network infrastructures behind Poco RAT and Bandook campaigns operated within the same **Autonomous Systems (AS).** This overlap reinforces the connection between the two malware families and their operators.

Table 5. AS overlap in campaigns

AS	Poco RAT	Bandook
200019, AlexHost SRL	185.216.68.121, 193.233.203.63	185.216.68.143, 194.48.248.72
44477, Stark Industries Ltd.	94.131.119.126	77.91.100.237, 45.67.34.219

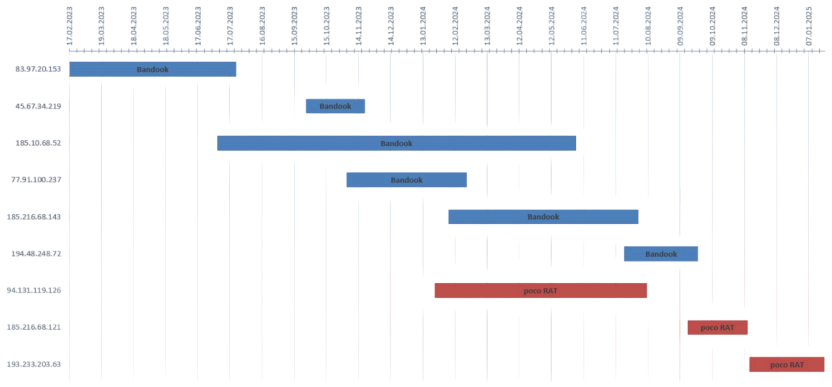

Figure 13. Network activity of C2 servers in Bandook and Poco RAT campaigns

The graph shows a clear pattern. As Bandook samples disappear, Poco RAT samples begin to surface, often using the same network infrastructure. The timing suggests more than just coincidence. Dark Caracal may have decided to swap out its old tool for something new.

Campaigns linked to Bandook and Poco RAT share a few signature traits. These include:

- Blurred decoy documents and link-shortening services
- Legitimate cloud storage services for payload distribution
- A focus on Spanish-speaking countries in Latin America
- Spanish-language content and financial transaction themes to make files look legitimate

PT Sandbox

YARA rules

apt_win_ZZ_DarkCaracal__Dropper__Bandook

Behavioral rules (malware)

Trojan.Win32.Inject.a
Trojan.Win32.Generic.a
Trojan-Downloader.Win32.PocoRAT.n

Behavioral rules (suspicious)

Create.Process.Inject.ResumeThread
Write.Process.Inject.SetThreadContext

MaxPatrol SIEM

Run_Masquerading_Executable_File
Suspicious_Connection
Suspicious_Connection_After_Imageload
Suspicious_File_Creation_From_Messenger_Or_Mail
Malicious_Office_Document

MITRE ATT&CK MATRIX

ID	Technique	Description
Resource Development		
T1608.001	Stage Capabilities: Upload Malware	Dark Caracal uses legitimate cloud storage platforms, such as Dropbox, Amazon, and Google Drive, to store its malware.
T1583.003	Acquire Infrastructure: Virtual Private Server	Dark Caracal rents and configures a VPS-based command-and-control (C2) server running Windows with an RDP interface, hosted outside Latin America. Preferred providers include Stark Industries Solutions Ltd. and AlexHost SRL.
T1588.001	Obtain Capabilities: Malware	Dark Caracal uses a lightweight RAT based on Bandook. The group uses obfuscated PDF and HTML documents as bait to lure victims.
Initial Access		
T1566.001	Phishing: Spearphishing Attachment	Dark Caracal sends phishing emails with lure documents containing links to download the malware.
Execution		

ID	Technique	Description
T1204.002	User Execution: Malicious File	The group manipulates victims into launching Poco RAT by exploiting themes of financial obligations to an organization the group is impersonating.
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Poco RAT uses the Windows command shell to execute remote commands.
Privilege Escalation		
T1055	Process Injection	Dark Caracal injects malicious Poco RAT code into legitimate Windows processes, such as cttune.exe and iexplore.exe.
Defense Evasion		
T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	Dark Caracal encrypts Poco RAT using the Twofish algorithm.
T1027.002	Obfuscated Files or Information: Software Packing	Dark Caracal uses UPX to pack Poco RAT.
T1055	Process Injection	Dark Caracal injects malicious code into legitimate Windows processes (cttune.exe and iexplore.exe).
Discovery		
T1082	System Information Discovery	Dark Caracal gathers detailed information about the infected system's operating system and hardware.
Command and Control		
T1132.001	Data Encoding: Standard Encoding	Dark Caracal exchanges encoded information about the infected system with the C2 server.
T1571	Non-Standard Port	Dark Caracal uses non-standard network ports (6541, 6542, 6543, 6211, 6212, and 6215) on the C2 server to manage infected hosts and extract data.
T1665	Hide Infrastructure	Dark Caracal uses URL shortening services, such as bit.ly, is.gd, ja.cat, and Rebrandly.

Network IoCs Poco RAT

ID	Purpose
94.131.119.126	C2 server
185.216.68.121	C2 server
193.233.203.63	C2 server

Network IoCs Bandook

ID	Purpose
83.97.20.153	C2 server
45.67.34.219	C2 server
185.10.68.52	C2 server
77.91.100.237	C2 server
185.216.68.143	C2 server
194.48.248.72	C2 server

MD5	SHA-1	SHA-256
a5073df86767ece0483da0316d66c15c	d0661df945e8e36aa78472d4b60e181769a3f23b	05bf7db7debfeb56702ef1b421a336d8431c3f7334
2a0f523b9e52890105ec6fbccd207dcd	f3a495225dc34cdeba579fb0152e4ccba2e0ad42	08552f588eafceb0fa3117c99a0059fd06882a36cc1
e0bf0aee954fd97457b28c9233253b0a	ce611811d9200613c1a1083e683faec5187a9280	0d6822c93cb78ad0d2ad34ba9057a6c9de8784f55
ec8746a1412d1bd1013dfe51de4b9fd1	f719b736ed6b3351d1846127afec8e0c68e54c1d	0fe11d78990590652f4d0f3afba5670e030b8ab714
fea98ca977d35828e294b7b9cc55fea9	63b4d283eaf367122ce0dec9fc0e586e63ef0c78	0ffc7ae741bb90c7f8e442d89b985def9969ebf2934
c41645cba3de5c25276650a2013cd32b	d8021edcb42b6472dded45f7a028aff6dfe5aaa6	121d941ba5a6ff8d99558e0919f49b926fbcd00e30
8778b9430947c46f68043666a71a2214	da3ea31e96fba64fcd840e930a99e705eb60c89b	12e849ffba407d5db756879fd257c4b736eb4b6ada
d8ec2df77a01064244f376322ba5aaf1	ce60069d5fdef4acced66e6fc049f351c465ee1e	13306775fdf506b706693deccb44ec364fe04dbf3c
bbfbd1ece4f4aa43d0c68a32d92b17e5	2ffdf164f6b8e2e403a86bd4d0f6260bf17fb154	1786f16a50a4255df8aa32f2e21f2829b4f8aaba2ce
32c6c0d29593810f69d7c52047e49373	4bf76e731d655f67c9e78a616cf8b21002a53406	18ba3612b1f0dbd23f8ab39b2d096bab0ed3438b3

Bandook

MD5	SHA1	SHA256
a2ea38d11bde2a4483b86321960d6319	5240860d0db91bd8e13a150676a3ab1917312c59	01e8536751080ea135c3ad7ae9187d06cdcccddfc
e6f23ff5f55bcb05669732c6a519a75a	6adc9cbcc5d3ce969d982f70728fd09ec3419a45	032ff087debc175342e01a3bb205fbd7ab2e724ba
27fabcf160575efc9ff6b7c93b35edd0	1d1f21745a5ea01cc3387099caae111a3cb79e6b	158255fa4a257953edf84323b4d7fef129ab55450
8fe826ceee2242238f918e7bba5ba7e7	06813b2b554db0de2aa296d31f951fd0cccda7bb	1e7d86f9ff5fd50aeeeb04040baad0ac0d84347d60
a12d326845a96a03867b2b70ca8f12ee	3b1264d2e156a09142847b6a18f70a3267c406e2	21ff46a6fc9173fcc147d7a5c603032c662c6c1f1b
40776099cf9098a626bae58763a503f6	43fc1530db54c356831f4fd96b81c1548c6b1a05	247b0725fc0935131537dd00eb454269f3dd5c8c5
abe2aa641f49f924a8c5bed6915b33a6	c02d9f23d6bf627b77e72cc55551aba15701945c	26ee4581ec0d064a1296e8178b016249977a483f
18d4b1fb0a643fa86e815a3464c48f65	8bddb48d29fb06b15a3314f2a1afc2839a22d5ce	302c707321abc9eca4d14171a33c9c5207711d2a1
5a21405b06a11ee03c24cc79ef910c3d	388371ea56bd79813ef53152220d7c64396528ea	3c099ec7363407c9fb742beca81f97ecca93807e0
812267e367c58c04d7c4800aa0f64603	dd75522dc6f64a9fa12723b8978cc682217056da	3cc284cecc3a8513d8ba664f88c1164312c049822

Decoy documents

MD5	SHA-1	SHA-256
2ecada671f172d4142e66e40d6d70b1b	2d30ce50578b95eed8feb093e0b8170a9d0b8994	918309457c875042e044510966083575a1635e977
b179ead57646353b0460a578f206c9af	256fca02ae02ffa70e6ea54e6cb43b877486ee6b	0864b87a18356bbe93b2e10f1deee5d4b705fc8248
5a4dd46d2eda27f97f88c2d4c5797114	4982c139f6627c991c426827088baf25f345ab97	57358c9f7f38a9364884cdcc4919ec3f7c71f147e43
26e11dfbfc87bed3a47099b0d4131868	617d867fcf5919a33c7b402ea85c6dbc03075fc3	e5ce11d9bdc7433f713a6f7bd1c05b0a98355ad8a9
a4a846ef5641949f1d6033537c719ffc	6fc2f4194e65dc8e4a29e71ca87ba3960df60fbe	a6ac2fd5dc59f5300c930b3fd5ffd6ed6e4dc27a270
f23043993fa2d4c4e4f04fb579c9745e	859c391e2181034eadc4d07ac1a58b73e358432d	8a0beec469a4373a2ebb4b21f013c33e3d2c539514
8daa10aa4ff65bb5e274a79df6aae004	b4c0700a6d325c439ca48c570c6736f6b3fce308	c8d20ae481f17de8606b92ab3170daea423081bf85
f5297dde39cda6b8423131af8f9220bd	11a892c4e2a67807ac161f9752a68f900dfb9b6a	289757c325556561c88a3918f3cc04251dc1d2fe2c
132a8a7c6a43ab61c6e9363f9c893905	baa2a99c0d53241324505d435908acf9506774d6	e5bc162807af900cf73a3f9a3e4cc1c5b10f774f44b
0c4f220e1c2fb895e0ca5cbdc17d202e	605c4887f774e2f25d9601beea26ac383cd25293	d633aeb1600c3d02bd21df94ee70fdf78d722e21df