ThreatCure

Cyber Threat Advisory

Poco RAT Campaign by Dark Caracal

Threat Actor Malware

Description

Poco RAT Campaign by Dark Caracal

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Data Theft and Espionage
- Financial Losses
- Operational Disruption
- Reputational Damage

Poco RAT malware, linked to the notorious threat group **Dark Caracal**, has been deployed in a targeted campaign against Spanish-speaking organizations, primarily in Latin America. Poco RAT is a sophisticated remote access Trojan (RAT) equipped with espionage capabilities, including file exfiltration, screenshot capture, command execution, and process manipulation.

Key Findings:

Malware Overview:

- Poco RAT is a backdoor that grants attackers full control over compromised systems.
- It uses the POCO C++ library for network communication and is packed with UPX to evade detection.
- The malware lacks built-in persistence, relying on external commands or secondary payloads for long-term access.

2. Attack Chain:

- **Initial Access:** Phishing emails with malicious attachments (PDF or HTML) impersonating financial documents.
- **Payload Delivery:** Victims are redirected to download a .rev archive from legitimate cloud storage services (e.g., Google Drive, Dropbox) or via link-shortening services (e.g., bit.ly).
- **Execution:** The dropper injects Poco RAT into legitimate processes (e.g., iexplore.exe, cttune.exe) to avoid detection.

Indicator of Compromise

IPs

94.131.119.126
185.216.68.121
193.233.203.63

MD5

a5073df86767ece0483da0316d66c15c
2a0f523b9e52890105ec6fbccd207dcd
e0bf0aee954fd97457b28c9233253b0a
ec8746a1412d1bd1013dfe51de4b9fd1
fea98ca977d35828e294b7b9cc55fea9
c41645cba3de5c25276650a2013cd32b
8778b9430947c46f68043666a71a2214
d8ec2df77a01064244f376322ba5aaf1
bbfbd1ece4f4aa43d0c68a32d92b17e5
32c6c0d29593810f69d7c52047e49373

SHA-1

d0661df945e8e36aa78472d4b60e181769a3f23b
f3a495225dc34cdeba579fb0152e4ccba2e0ad42
ce611811d9200613c1a1083e683faec5187a9280
f719b736ed6b3351d1846127afec8e0c68e54c1d
63b4d283eaf367122ce0dec9fc0e586e63ef0c78
d8021edcb42b6472dded45f7a028aff6dfe5aaa6
da3ea31e96fba64fcd840e930a99e705eb60c89b
ce60069d5fdef4acced66e6fc049f351c465ee1e
2ffdf164f6b8e2e403a86bd4d0f6260bf17fb154
4bf76e731d655f67c9e78a616cf8b21002a53406

SHA-256

05bf7db7debfeb56702ef1b421a336d8431c3f7334187d2ccd6ba34816a3fd5a
08552f588eafceb0fa3117c99a0059fd06882a36cc162a01575926736d4a80eb
0d6822c93cb78ad0d2ad34ba9057a6c9de8784f55caa6a8d8af77fed00f0da0a
0fe11d78990590652f4d0f3afba5670e030b8ab714db9083fd0a981e0f1f48f3
0ffc7ae741bb90c7f8e442d89b985def9969ebf293442f751ab2e69f4df226a8
121d941ba5a6ff8d99558e0919f49b926fbcd00e3007aad14ac85e799d55473c
12e849ffba407d5db756879fd257c4b736eb4b6adac6320d2f1916d6a923fa46
13306775fdf506b706693deccb44ec364fe04dbf3c471227c2439c2462e19080
1786f16a50a4255df8aa32f2e21f2829b4f8aaba2ced3e4a7670846205b3ac70
18ba3612b1f0dbd23f8ab39b2d096bab0ed3438b37932f473c787e24e57e8397

Remediation

- Email Security:
    - Implement advanced email filtering to detect and block phishing emails.
    - Train employees to recognize suspicious emails and avoid opening unexpected attachments.
- Network Monitoring:
    - Block traffic to known C2 IP addresses and monitor for unusual outbound connections.
    - Use intrusion detection systems (IDS) to identify suspicious network activity.
- User Awareness:
    - Conduct regular cybersecurity training to educate employees about phishing tactics.
    - Encourage reporting of suspicious emails or files.
- Incident Response:
    - Develop and test an incident response plan to quickly contain and remediate infections.
    - Isolate compromised systems and conduct forensic analysis to identify the scope of the breach.

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Secure your byte world

Poco RAT Campaign by Dark Caracal

Threat Actor Malware

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE