



ThreatCure
Cyber Threat Advisory
PhantomCore

Threat Actor Malware



Description

PhantomCore

CATEGORY

Malware

SEVERITY

High



Platforms

Windows, Linux

IMPACT

- Operational Disruption
- Data Breaches
- Economic and Reputational Damage

PhantomCore, a cyber threat group, is currently active in Pakistan and the broader Asian region, where it deploys PhantomRAT, a remote access trojan, through phishing emails. These emails, which look legitimate and often use official logos, include a password-protected RAR file as an attachment. The archive leverages a vulnerability (CVE-2023-38831) in older versions of WinRAR, causing a hidden .NET executable to run when the victim attempts to open an innocuous-looking PDF file. This executable installs PhantomRAT, granting attackers extensive control over the system for actions like file theft, credential harvesting, activity monitoring, and remote command execution. While similar RAR-based attack strategies have been seen in other groups, PhantomCore's exact origins remain uncertain, with limited visibility in some regional networks.



Kill Chain

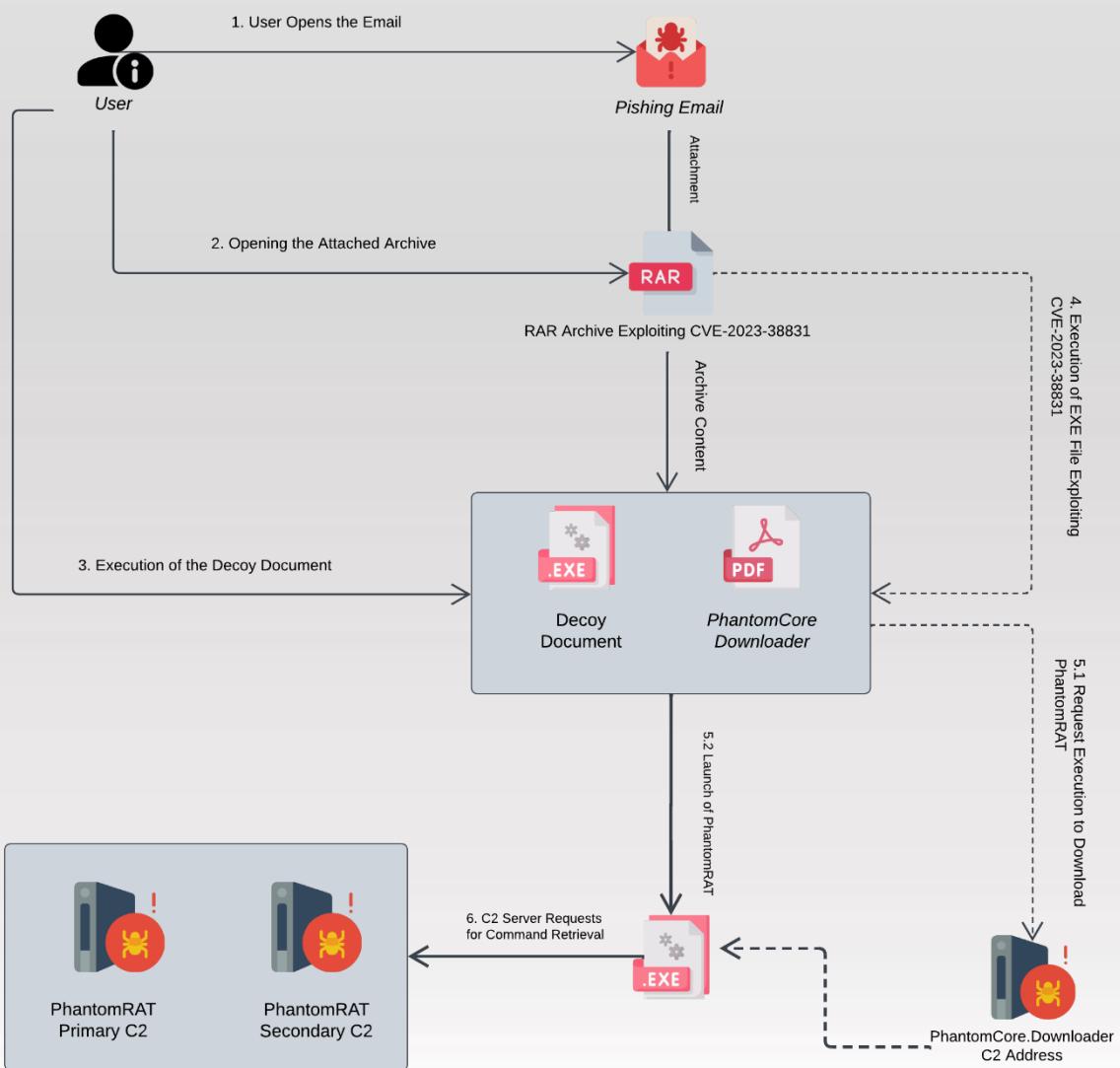
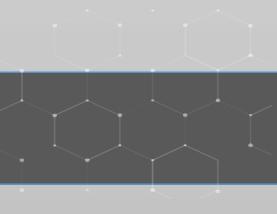


Figure 1 Kill Chain

Indicator of Compromise

SHA256

```
201F8DD57BCE6FD70A0E1242B07A17F489C5F873278475AF2EAF82A751C24FA8
9F5B780C3BD739920716397547A8C0E152F51976229836E7442CF7F83ACFDC69
08DC76D561BA2F707DA534C455495A13B52F65427636C771D445DE9B10293470
6A889F52AF3D94E3F340AFE63615AF4176AB9B0B248490274B10F96BA4EDB263
33786D781D9C492E17C56DC5FAE5350B94E9722830D697C3CBD74098EA891E5A
5D924A9AB2774120C4D45A386272287997FD7E6708BE47FB93A4CAD271F32A03
9B005340E716C6812A12396BCD4624B8CFB06835F88479FA6CFDE6861015C9E0
5A3C5C165D0070304FE2D2A5371F5F6FDD1B5C964EA4F9D41A672382991499C9
DC3E4A549E3B95614DEE580F73A63D75272D0FBA8CA1AD6E93D99E44B9F95CAA
053BA35452EE2EA5DCA9DF9E337A3F307374462077A731E53E6CC62EB82517BD
2F9B3C29ABD674ED8C3411268C35E96B4F5A30FABE1AE2E8765A82291DB8F921
015A6855E016E07EE1525BFB6510050443AD5482039143F4986COE2AB8638343
9D056138CFB8FF80B0AA53F187D5A576705BD7954D36066EBBF34A44326C546
22898920DF011F48F81E27546FECE06A4D84BCE9CDE9F8099AA6A067513191F3
2F1EE997A75F17303ACC1D5A796C26F939EB63871271F0AD9761CDBD592E7569
AF5A650BF2B3A211C39DCDCAB5F6A5E0F3AF72E25252E6C0A66595F4B4377F0F
9E9FABBA5790D4843D2E5B027BA7AF148B9F6E7FCDE3FB6BDDC661DBA9CCB836
B8447EF3F429DAE0AC69C38C18E8BDBFD82170E396200579B6B0EFF4C8B9A984
92804FAAAB2175DC501D73E814663058C78COA042675A8937266357BCFB96C50
664B68F2D9F553CC1ACFB370BCFA2CCF5DE78A11697365CF8646704646E89A38
311EDF744C2E90D7BFC550C893478F43D1D7977694D5DCECF219795F3EB99B86
4C218953296131D0A8E67D70AEEA8FA5AE04FD52F43F8F917145F2EE19F30271
2D3DB0FF10EDD28EE75B7CF39FCF42E9DD51A6867EB5962E8DC1A51D6A5BAC50
DC47D49D63737D12D92FBC74907CD3277739C6C4F00AAA7C7EB561E7342ED65E
EDA18761F3F6822C13CD7BEAE5AF2ED77A9B4F1DC7A71DF6AB715E7949B8C78B
```



Indicator of Compromise

| MD5

```
15333d5315202ea428de43655b598eda
55239cc43ba49947bb1e1178fb0e9748
76b23dd72a883d8b1302bb4a514b7967
6ddc56e77f57a069539dcc7f97064983
7acc6093d1bc18866cdd3feccb6da26a
0e14852853f54023807c999b4ff55f64
99b0f80e9ae2f1fb15bfe5f068440ab8
2799415007628a4647071aeadfbf007a
2525b41e278337b320eb773dad7949fd
16f97ec7e116fe3272709927ab07844e
5d8d727a376b8bee36ee2aef918540bb
b39b8c18a294240eb284787f07206b67
07db05ee98e9284a52f767b6410acdd7
0e763512095abc4616f81cf4631b9b2f
9a72cde58feed74a4ea301d6ddf41fd4
2e2da33b244a4bd17d5ddfb7f29b8b22
e930b05efe23891d19bc354a4209be3e
76b23dd72a883d8b1302bb4a514b7967
e74f35cc8b41c77a75ed5bfc867344c8
```



Remediation

1. User Awareness and Training

Train employees to recognize phishing tactics and handle suspicious emails cautiously.

2. Update and Patch Management

Regularly update software, especially tools like WinRAR, to close vulnerabilities.

3. Email Security Controls

Use email filtering to block phishing attempts and malicious attachments.

4. Endpoint Detection and Response (EDR)

Deploy EDR solutions to detect and respond to malicious activity on endpoints.

5. File Integrity Monitoring

Monitor critical files for unexpected changes that could indicate malware activity.

6. Restrict Privileges

Limit user permissions to reduce the impact of malware if it executes.

7. Network Security Measures

Use firewalls and IDS/IPS to detect and block suspicious network traffic.

8. Monitoring and Logging

Regularly review logs for signs of phishing, unauthorized downloads, or abnormal traffic.

9. Incident Response Plan

Establish and test a response plan for quick containment and recovery from attacks.

10. Backup and Recovery

Keep regular, offline backups to ensure data can be restored if compromised.

ThreatCure

Cyber Threat Advisory

Secure your byte world



PhantomCore

Threat Actor Malware

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

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

Get Started Today

**THREAT
CURE**
RE-ARCHITECT YOUR THREAT LANDSCAPE