ADVISORY FOR ICM SECTOR

# GLACIAL PANDA Profile

Original report published on: May 28, 2025

## Executive Summary

CrowdStrike attributed GLACIAL PANDA for targeting Linux-based systems within telecommunications networks, primarily across Asia and North America since 2018. The group employs living-off-the-land (LOTL) tactics and exploits legitimate user accounts to gain initial access, conduct lateral movement and maintain persistence within affected environments. These advanced methods make eradication difficult, requiring thorough and sustained remediation efforts.

## Background

In September 2018, GLACIAL PANDA exploited the DIRTYCOW vulnerability (CVE-2016-5195) to gain SSH authentication and escalate privileges to root on a targeted host. Following initial access, the adversary employed common TTPs against Unix and Linux systems, including host reconnaissance, lateral movement using netcat and persistence through the installation of backdoors. GLACIAL PANDA deployed trojanised OpenSSH server and binaries designed to capture and log credentials to files stored in unique locations.

In April 2022, after an unsuccessful attempt to re-exploit the DIRTYCOW vulnerability, GLACIA PANDA transferred a file name CVE-2021-4034-centos6.9.tar.bz2 to the host. They extracted and compiled a binary likely intended to exploit the PwnKit vulnerability (CVE-2021-4034) in the Linux polkit's pkexec[1] utility. Exploiting this vulnerability allows arbitrary code execution and privilege escalation.

The group has reportedly accessed and likely exfiltrated sensitive call detail records and communication telemetry from multiple telecom operators, posing significant privacy risks to subscribers. There is no evidence at this time of GLACIAL PANDA altering telecom protocols or intercepting communications directly.

## Detection and Mitigation

IMDA recommends organisations to perform continual testing and validation of existing security controls to ensure detection and prevention against the DIRTYCOW malware and shell script identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
  - Create, test and validate detection rules against the threat behaviours.
  - Validate and deny/disable processes, ports and protocols that have no business need.
- Enable logging of SSH connections between hosts and monitor for anomalies.
- Implement multi-factor authentication (MFA) organisation-wide to reduce the risk of credential misuse
- Enforce network access control list based on host roles and responsibilities.
- Conduct regular audits of user accounts and promptly remove any that are no longer required.
- Validate and add malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR).

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

**Annex A - Indicators of Compromise**

| SHA256 Hash | Description |
|---|---|
| 5b5b38f76c2c20274fb9f1c5c325372d4482f0ce85c3f77c94d0586cc51de829 | Trojanized SSH binary |
| 63de0cf0d2bf65d39ecf4bc6d2b7fe4fe348428e8413c0dcc0e307f56d52ca0d | Trojanized SSH binary |
| 1a26badb0356545b508c9215827ee244b9b90b310c3edcc95e9a4b33fb819563 | Trojanized SSHD binary |
| 875f3dfb026b7ef792800b129527fc99c24c0c9b22bd8c97d775dfcd0987c275 | Trojanized SSHD binary |
| 60e04b334fc864b6dffc3438ab7009abeca20dbe4ca89e041d6f8b8c8e5f440f | Trojanized SSH PAM |
| 74c9780758a10dfef0d7acb6cce489daa80d657a307a2743621df67e02b976b9 | Trojanized SSH PAM |
| 1ee367972da4dc6dc72cb75867fef407d9ef36bdba5296f1e67ac6221088dc5e | Trojanized crond binary |
| 9472585f157fbb6193139e1b1344d002d0eb655f36a6290da978a8b1b1c283e2 | Trojanized crond binary |
| 7fc0d0c79f1090ec7ad0987fb176e6321406e37a4287de8d28c0c85bb07a7e30 | Reverse Shell Perl Scripts |
| 752c5ccb83cbf98653a97385b2ae195a84cb2c916dddbf8e44f981b5d78513be | Reverse Shell Perl Scripts |

| IP Address | Description |
|---|---|
| 202[.]181[.]247[.]135 | Reverse Shell Network |
| 140[.]113[.]39[.]16 | |
| 163[.]22[.]7[.]60 | |
| 167[.]99[.]29[.]33 | |
| 163[.]22[.]7[.]52 | |
| 167[.]99[.]68[.]210 | |
| 60[.]251[.]42[.]155 | |
| 120[.]127[.]18[.]212 | |
| 140[.]136[.]208[.]25 | |
| 59[.]120[.]51[.]115 | |
| 220[.]130[.]89[.]220 | |
| 206[.]189[.]157[.]64 | GLACIA PANDA Support Infrastructure |
| 45[.]116[.]82[.]62 | |

**Annex B - MITRE ATT&CK Tactics and Techniques**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Reconnaissance | T1595 | Active Scanning |
| | T1595.002 | Active Scanning: Vulnerability Scanning |
| Resource Development | T1583.003 | Acquire Infrastructure: Virtual Private Server |
| | T1584.004 | Compromise Infrastructure: Server |
| | T1587.001 | Develop Capabilities: Malware |
| | T1588.002 | Obtain Capabilities: Tool |
| | T1588.005 | Obtain Capabilities: Exploits |
| | T1608.002 | Stage Capabilities: Upload Tool |
| Initial Access | T1190 | Exploit Public-Facing Application |
| | T1199 | Trusted Relationship |
| | T1078 | Valid Accounts |
| Execution | T1059 | Command and Scripting Interpreter |
| | T1059.004 | Command and Scripting Interpreter: Unix Shell |
| | T1053.003 | Scheduled Task/Job: Cron |
| Persistence | T1554 | Compromise Host Software Binary |
| | T1556.003 | Modify Authentication Process: Pluggable Authentication Modules |
| | T1053.003 | Scheduled Task/Job: Cron |
| | T1078 | Valid Accounts |
| Privilege Escalation | T1548 | Abuse Elevation Control Mechanism |
| | T1548.001 | Abuse Elevation Control Mechanism: Setuid and Setgid |
| | T1068 | Exploitation for Privilege Escalation |
| | T1078 | Valid Accounts |
| Defence Evasion | T1564 | Hide Artifacts |
| | T1070.002 | Indicator Removal: Clear Linux or Mac System Logs |
| | T1070.006 | Indicator Removal: Timestomp |
| | T1078 | Valid Accounts |
| Credential Access | T1555 | Credentials from Password Stores |
| | T1056 | Input Capture |
| | T1556.003 | Modify Authentication Process: Pluggable Authentication Modules |
| | T1003.008 | OS Credential Dumping: /etc/passwd and /etc/shadow |
| | T1649 | Steal or Forge Authentication Certificates |
| Discovery | T1654 | Log Enumeration |
| | T1018 | Remote System Discovery |
| | T1082 | System Information Discovery |
| | T1049 | System Network Connections Discovery |
| Lateral Movement | T1570 | Lateral Tool Transfer |
| | T1021.004 | Remote Services: SSH |
| Collection | T1560.001 | Archive Collected Data: Archive via Utility |
| | T1213 | Data from Information Repositories |
| | T1005 | Data from Local System |
| | T1074.001 | Data Staged: Local Data Staging |

| | | |
|---|---|---|
| | T1056 | Input Capture |
| Command and Control | T1071 | Application Layer Protocol |
| | T1571 | Non-Standard Port |
| Exfiltration | T1041 | Exfiltration Over C2 Channel |
| Impact | T1565.001 | Data Manipulation: Stored Data Manipulation |

**References**

1. ^ Polkit (also known as PolicyKit), developed RedHat, manages access control on Unix-like systems, allowing unprivileged processes to communicate with privileged ones. Pkexec utility lets authorised user to run commands as another user, defaulting to root if none is specified.