



THREAT ADVISORY

Operation RapidRust: APT36 Deploys Sophisticated Rust-Based Malware



PREPARED BY

Drona Cyber Solutions Pvt Ltd

DATE OF ISSUE

September 18, 2026

CLASSIFICATION MATRIX

TLP : GREEN

1. EXECUTIVE OVERVIEW & CAMPAIGN THREAT PROFILE

An advanced cyber espionage campaign identified as **Operation RapidRust** has been observed targeting high-value defense, aerospace, law enforcement, and government organizations[cite: 1]. The campaign is formally attributed to the Pakistan-nexus nation-state threat actor **APT36**[cite: 1]. The observed operational activity demonstrates a significant leap in threat-actor sophistication, marked by complete architectural migration to compiled memory-safe languages, stealthy cloud API-based Command and Control (C2), and intentional operational capability designed to breach strictly isolated air-gapped mission environments[cite: 1].

Campaign Identifier	Operation RapidRust[cite: 1]	Primary Motivation	State-Sponsored Espionage / Strategic Intelligence Exfiltration
Threat Actor Profile	APT36 (Pakistan-Nexus)[cite: 1]	Threat Landscape Impact	Targeted operations against Indian & Afghan defense infrastructure[cite: 1]
Malware Arsenal	RUSTYSHADE (Backdoor), RUSTYMOVE (Air-Gap Traversing Worm), PSNATCH (Win Stealer), BASHNATCH (Linux Stealer)[cite: 1]		
Infrastructure Pattern	Legitimate Cloud Repositories (GitHub API)[cite: 1], Cloud Storage (Backblaze B2), Typosquatted Domains impersonating national press agencies.		

STRATEGIC RISK ASSESSMENT

The shift to compiled Rust code substantially neutralizes traditional static signature defenses. Coupled with removable media propagation vectors explicitly designed to bypass perimeter air-gaps[cite: 1], this operation targets deep enterprise core enclaves and offline mission networks. Immediate threat-hunting and credential rotations are strongly advised.

2. DEPLOYED MALWARE ARSENAL

The threat actor replaced legacy commodity payloads with a custom-engineered, multi-tier arsenal[cite: 1]:

- RUSTYSHADE (Command & Control Backdoor):** A modular 64-bit Windows implant written in Rust. Avoids direct socket connections by leveraging the private GitHub REST API as its command-and-control conduit. Commands are ingested via `command.txt`, while exfiltrated results and system telemetry are published to `results.txt` and `screenshot.png`.
- RUSTYMOVE (Air-Gap Lateral Traverser):** A dedicated Rust-based worm engine engineered to propagate payloads across segregated, air-gapped networks[cite: 1]. It continuously monitors host disk subsystems for removable media insertions, immediately staging a weaponized payload package containing `DriverInstaller.zip` (carrying RUSTYSHADE) paired with a deceptive `.LNK` shortcut.
- PSNATCH & BASHNATCH (Targeted File Exfiltrators):** Highly automated file stealers developed in PowerShell (for Windows targets) and Bash (for Linux deployments)[cite: 1]. They recursively harvest files across local drives and attached external storage modified within the past 120 days, tracking exfiltration state via local JSON caches to avoid duplicate network traffic.

3. IN-DEPTH TECHNICAL ANALYSIS & ATTACK MECHANICS

GITHUB API COMMAND & CONTROL CHANNEL

RUSTYSHADE eschews conventional dynamic DNS or VPS-hosted C2 servers. Instead, it uses legitimized outbound HTTPS requests targeting private GitHub repositories using an embedded Personal Access Token (PAT). All payload transmissions are encrypted end-to-end via **AES-256-GCM**, utilizing a key derived from the SHA-256 hash of the PAT. Encrypted payloads are Base64-encoded and marked with an identifying header prefix **HCENCI:**.

```
// GitHub REST API Integration Template utilized by RUSTYSHADE
Endpoint: https://api.github.com/repos/[owner]/[repo]/contents/[path]?ref=[branch]&t=[timestamp]
Authentication: Authorization: token [PAT]
Accept Header: application/vnd.github.v3+json
Exfiltration User-Agent: SmartUploader
```

AIR-GAP CROSSING ENGINE (RUSTYMOVE DRIVE DETECTION)

RUSTYMOVE leverages direct PowerShell execution wrappers to interrogate partition architectures and target removable drives across hardware buses (e.g., USB, 1394, SD, MMC):

```
powershell.exe -NoProfile -NonInteractive -WindowStyle Hidden -Command "
Get-Volume | Where-Object DriveLetter | ForEach-Object {
    $letter = $_.DriveLetter
    $part = Get-Partition -DriveLetter $letter -ErrorAction SilentlyContinue
    if (-not $part) { return }
    $disk = Get-Disk -Number $part.DiskNumber -ErrorAction SilentlyContinue
    if (-not $disk) { return }
    $external = ($disk.BusType -in @('USB', '1394', 'SD', 'MMC')) -or
                ($disk.MediaType -in @('Removable Media', 'External hard disk media'))
    if ($external -and $_.UniqueId) {
        Write-Output ('{0}:{1}' -f $letter, $_.UniqueId)
    }
}"
```

OPERATOR PROFILE, RECONNAISSANCE, AND STAGING INFRASTRUCTURE

Forensic analysis reveals rigid operational windows. Threat actor command executions were recorded strictly between **04:00 UTC and 11:00 UTC**, operating exclusively on **weekdays** with no registered weekend activity. This cadence reflects state-sponsored shifts within standard regional military-bureaucratic office hours.

Following foothold establishment, the actor systematically executes native utility sweeps (`whoami`, `ipconfig`, `arp -a`, `tasklist`). Port scanning is directed against SMB (445) and RPC (135) for lateral movement over IPC\$ admin shares. Intermediate PowerShell stages are hosted on typosquatted domains masquerading as Indian press publications (e.g., `theprints[.]org`, `indiatodays[.]org`).

4. MITRE ATT&CK MATRIX ALIGNMENT

TACTIC	TECHNIQUE ID	TECHNIQUE DESCRIPTION
Execution	T1059.001 / .003	Execution via PowerShell & Windows Command Shell
Persistence	T1053.005	Scheduled Task (<code>StandAloneOneDriveUpdater-2626</code>)
Defense Evasion	T1070.004	Indicator Removal: Tool Deletion and File Renaming
Discovery	T1046 / T1135	Network Service Scanning (SMB/RPC) & Local Share Discovery
Lateral Movement	T1091 / T1021.002	Replication via Removable Media & SMB/Admin Shares
Collection	T1005 / T1113	Automated Local Data Ingestion & Periodic Screen Capture
Command & Control	T1102.002 / T1573	Bidirectional GitHub REST API abuse; Symmetric AES-256-GCM

5. INDICATORS OF COMPROMISE (IOCS)

INDICATOR TYPE	VALUE / OBSERVABLE STRING
Malicious Domains	<code>theprints[.]org</code> <code>indiatodays[.]org</code> <code>officialinfo[.]org</code> <code>f005[.]backblazeb2[.]com</code>
Malicious URLs	<code>http[:]//theprints[.]org/adrive</code> <code>/drivefolder</code> <code>/msheets</code> <code>/gsheets</code> <code>https[:]//clients-easy[.]js3[.]us-east-005[.]backblazeb2[.]com/Automata-20[.]zip</code> <code>https[:]//f005[.]backblazeb2[.]com/file/Clients-easy/DriverInstaller[.]zip</code>
File Hashes (SHA-256)	<code>52d07b3ef0c5f27d082551d51027de452682e1fbd5bb38a897ea4b31bd387523</code> <code>80fdde0dafa450ae33937cce752b46666da567926b2f39b37e02e77f9d6a92e</code> <code>70fc6cba3c2021889fb4093d0221dc6925818666df25718a630c562cac18da31</code> <code>05bbeea42f481a3dd1b3f670aba481f7c5c8e897ef321d65188317be5a65a4d7</code>

6. STRATEGIC REMEDIATION ROADMAP

1. USB Storage Restriction & Endpoint Media Isolation	CRITICAL PRIORITY
Enforce centralized Group Policy Objects (GPO) to strictly disable removable drive autorun features. Mandate real-time behavioral malware scans on peripheral insertion and restrict execution access from external storage devices.	
2. PowerShell & Script Execution Hardening	CRITICAL PRIORITY
Enforce PowerShell Constrained Language Mode (CLM) along with AppLocker/WDAC application control policies to block untrusted script execution. Ensure Script Block Logging (Event ID 4104) is enabled across all endpoints.	
3. Cloud API & GitHub Egress Filtering	HIGH PRIORITY
Inspect and restrict corporate egress traffic reaching GitHub API endpoints. Monitor for non-standard User-Agents such as <code>SmartUploader</code> and alert on anomalous PAT token generation in enterprise code repositories.	
4. Persistence Auditing & Micro-Segmentation	MEDIUM PRIORITY
Continuously audit Scheduled Tasks for anomalous naming conventions like <code>StandAloneOneDriveUpdater-2626</code> . Enforce micro-segmentation to restrict SMB (TCP 445) and RPC (TCP 135) east-west traffic between workstations.	



**Securing Today,
Empowering Tomorrow**



Drona Cyber Sloutions



info@dronacybersolutions.com



+91 81609 68270



www.dronacybersolutions.com