ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Web Defacement Artifacts on Bangladesh Government Infrastructure Potentially Linked to Global Magento Exploitation Campaign

TLP: CLEAR
Distribution: Public
Advisory on: Web Defacement Artifacts on Bangladesh Government Infrastructure Potentially Linked to Global Magento Exploitation Campaign
Severity: High
Threat Type: Website Defacement / Remote Code Execution / Unauthorized File Upload
Date: 03 May 2026

Executive Summary

Cyber Threat Intelligence Unit of BGD e-Gov CIRT has identified multiple Bangladesh government web domains hosting suspicious artifact files such as **gc.txt** and **uname.txt** in publicly accessible directories. These files are commonly used by threat actors to verify unauthorized write access to web servers and claim defacement activities.

The observed artifacts coincide with indicators associated with a large-scale global web defacement campaign targeting **Magento infrastructure**, first reported on 27 February 2026. The campaign has resulted in the compromise of more than **15,000 hostnames** across approximately **7,500 domains worldwide**.

Technical analysis suggests attackers may be exploiting unauthenticated file upload vulnerabilities or remote code execution flaws in vulnerable web applications, allowing arbitrary files to be written to web directories. Although attribution remains unconfirmed, the observed artifacts match patterns reported in the global campaign where attackers uploaded plaintext files and subsequently reported compromised sites to public defacement archives.

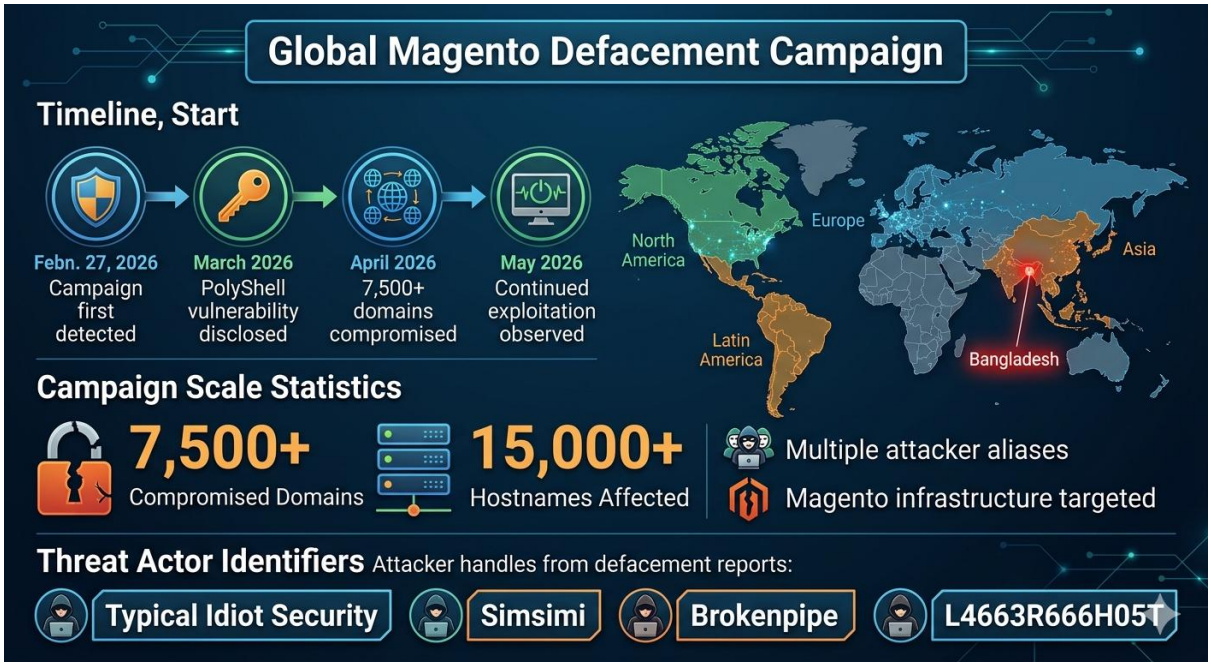

Figure: Global Distribution of the Magento Defacement Campaign

Observed Indicators in Bangladesh

Threat intelligence monitoring detected several government infrastructure endpoints hosting unauthorized files.

URL	Artifact
https://***cpanel.***.gov.bd/gc.txt	Defacement claim file
https://portal.*******.gov.bd/gc.txt	Defacement artifact
http://server***.*******.gov.bd/gc.txt	Defacement artifact
http://****.gov.bd/uname.txt	System verification artifact
https://****.gov.bd/uname.txt	System verification artifact

Observed Artifact Behavior: These files typically contain:

- attacker handles or aliases
- timestamps
- proof-of-compromise text
- server verification output

Such artifacts are often used by attackers to:

- confirm successful exploitation
- demonstrate file system write access
- provide evidence for submission to defacement archives such as **Zone-H**

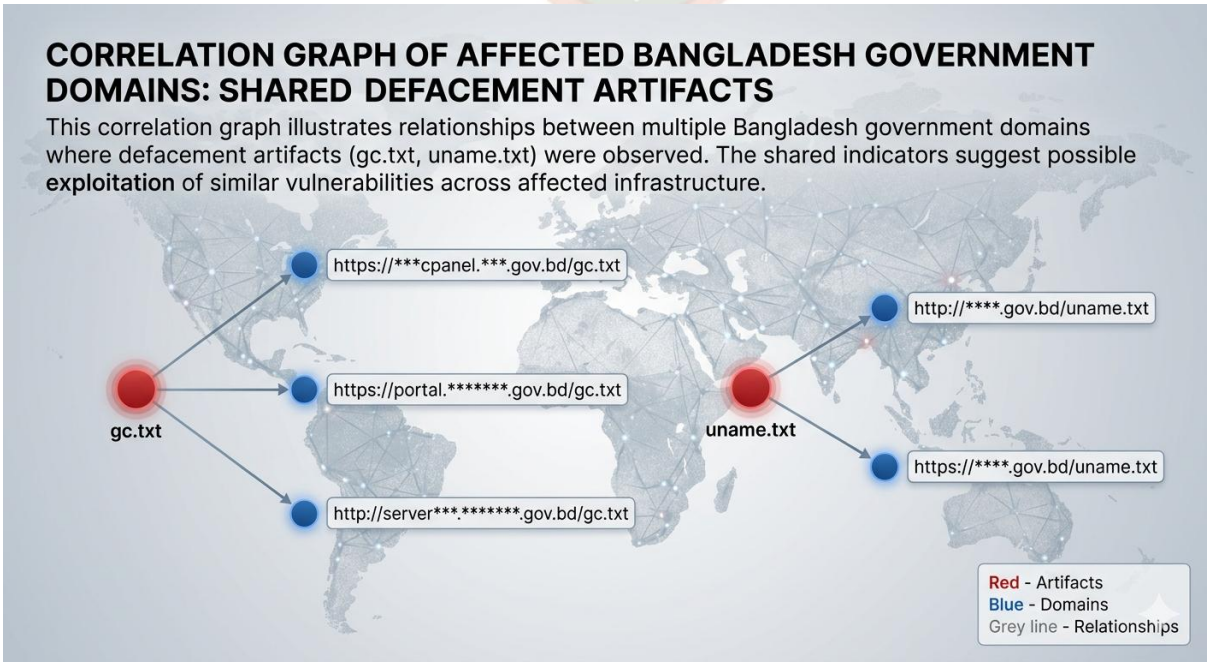

Figure: Correlation Graph of Web Defacement Artifacts Across Bangladesh Government Domains

Global Threat Context

Security researchers have documented a large-scale defacement campaign targeting Magento servers globally. Most defacements were reported to **Zone-H**, suggesting reputation-building activity within the defacement community. Key campaign characteristics include:

- compromise of 7,500+ domains
- more than 15,000 affected hostnames
- exploitation of vulnerable Magento REST API endpoints
- plaintext defacement artifacts uploaded to web directories

Threat actors involved in the campaign have used aliases including:

- *Typical Idiot Security*
- *L4663R666H05T*
- *Simsimi*
- *Brokenpipe*

Technical Root Cause Analysis

PolyShell Vulnerability (APSB25-94): The campaign has been linked to the PolyShell vulnerability, affecting Magento Open Source and Adobe Commerce.
Vulnerability Type: Unauthenticated Arbitrary File Upload
Affected Component: Magento REST API file upload functionality

Attack Mechanism: The vulnerability allows attackers to upload files encoded in base64 format through REST API endpoints without proper validation.

Example attack workflow:

```
POST /rest/V1/products
Content-Type: application/json
```

Malicious payload example:

```
{
  "file": "base64_encoded_payload"
}
```

If server-side validation is misconfigured, the uploaded payload can be written to the filesystem.

Potential Outcome:

- Arbitrary file upload
- Web shell deployment
- Remote code execution
- Full server compromise

SessionReaper Vulnerability (CVE-2025-54236): Another vulnerability observed in similar campaigns is SessionReaper, a critical Magento RCE flaw.

CVSS Score: 9.1 (Critical)

Vulnerable Endpoint: `/customer/address_file/upload`

Exploitation Mechanism: The vulnerability exploits nested deserialization flaws, allowing attackers to execute arbitrary code via crafted payloads.

Attack Chain Reconstruction

The attack pattern observed in the global campaign typically follows the sequence below.

Stage 1 — Internet-wide Scanning:

Attackers scan for vulnerable Magento installations. Common scanning targets:

- `/rest/V1/` [Magento REST API]
- `/customer/address_file/upload` [File upload endpoint]
- `/pub/media/` [Public media directory]

Stage 2 — Exploitation:

Attackers send crafted requests exploiting file upload vulnerabilities. Possible uploaded files include:

- web shells
- PHP backdoors
- plaintext defacement artifacts

Stage 3 — Filesystem Write Access:

Attackers upload files such as: (These files are stored in publicly accessible directories.)

- `gc.txt`
- `uname.txt`
- `shell.php`

Stage 4 — Proof of Compromise:

Attackers verify access by retrieving uploaded artifacts through HTTP requests.

Example: `GET /gc.txt`

Stage 5 — Public Defacement Claim:

The attacker reports the compromised domain **to Zone-H or similar defacement archives**.

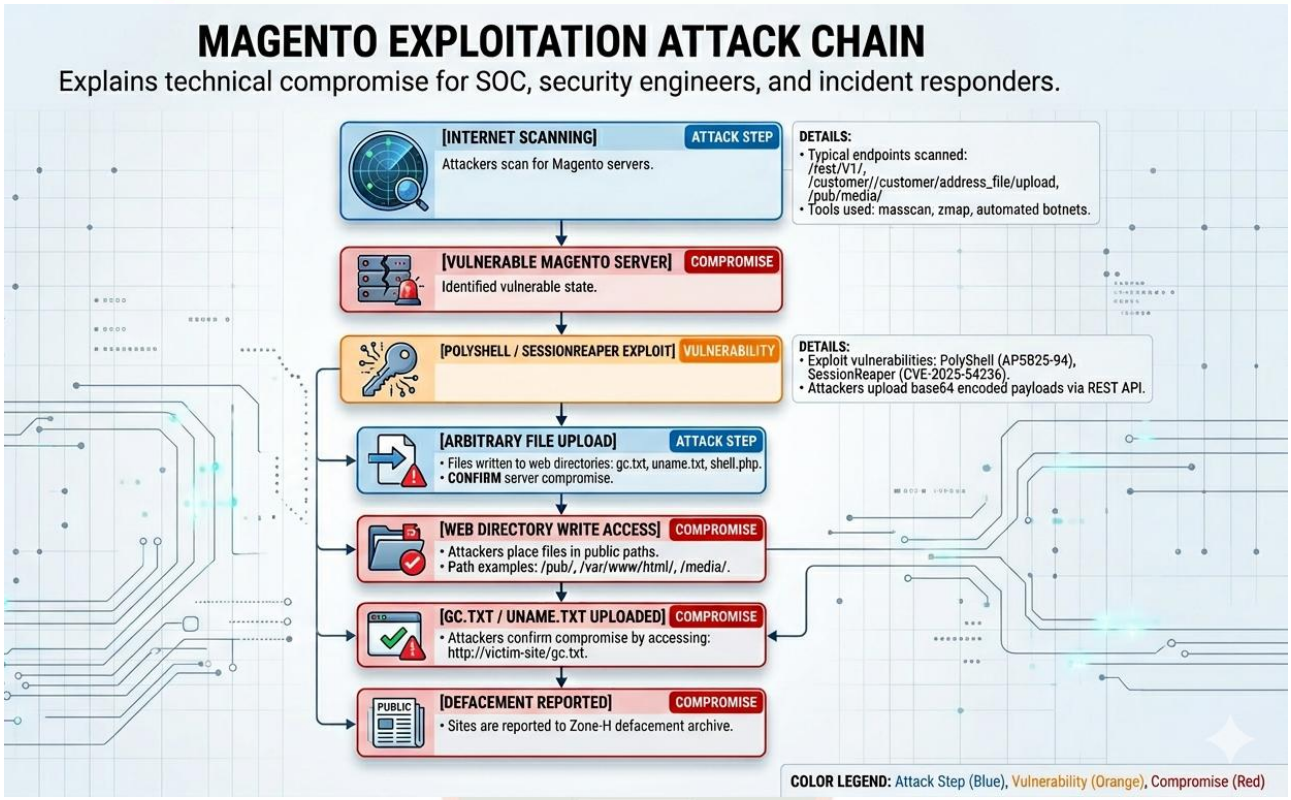

Figure: Magento Exploitation Attack Chain

Potential Impact

If exploitation is confirmed, attackers may gain:

- persistent web server access
- ability to upload additional payloads
- access to sensitive application data
- ability to modify web content

Possible consequences include:

- website defacement
- customer data exposure
- payment card skimming
- malware hosting

MITRE ATT&CK Mapping

Technique	ID	Description
Exploit Public-Facing Application	T1190	Exploiting Magento vulnerabilities
Command Shell	T1059	Execution of uploaded scripts
Web Shell	T1505.003	Persistent server access
Defacement	T1491	Unauthorized modification of website content

Recommended Immediate Actions

Incident Response:

- remove unauthorized files (`gc.txt, uname.txt`)
- perform full filesystem integrity check
- investigate web server logs
- search for web shells

Application Security:

- patch Magento installations
- disable unused REST API endpoints
- enforce strict file upload validation
- restrict write access to web directories

Monitoring and Detection:

SOC teams should monitor for indicators such as:

```
GET /gc.txt
GET /uname.txt
POST /rest/V1/
POST /customer/address_file/upload
```

Example web server log detection rule:

```
uri_path contains ".txt"
AND response_size < 5KB
AND uri_path in ("gc.txt","uname.txt")
```

SIEM detection example:

```
index=web_logs
| search uri="/gc.txt" OR uri="/uname.txt"
```