ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

TerminalFix Campaign: ClickFix-Based Multistage Intrusion Deploying Reverse Tunneling and Active Directory Reconnaissance

TLP: CLEAR
Distribution: Public
Advisory on: TerminalFix Campaign: ClickFix-Based Multistage Intrusion Deploying Reverse Tunneling and Active Directory Reconnaissance
Severity: High
Threat Type: Social Engineering, PowerShell Execution, DLL Side-Loading, Steganography, Persistence, Active Directory Reconnaissance, Reverse Tunneling
Target Environment: Windows Enterprise, Government, Critical Infrastructure and Domain-Joined Networks
Primary Risk: Compromised endpoint converted into an internal network pivot
Date: 02 September 2026

Executive Summary

The Cyber Threat Intelligence (CTI) Unit of BGD e-GOV CIRT is issuing this advisory regarding the recently observed **TerminalFix campaign**, a sophisticated evolution of the ClickFix social-engineering technique.

The campaign begins with a compromised website displaying a fraudulent Cloudflare CAPTCHA/Turnstile verification interface. Instead of performing a genuine CAPTCHA verification, the victim is instructed to copy and paste a command into Windows Terminal or PowerShell. Once executed, the command initiates a multistage intrusion involving PowerShell, DLL side-loading, steganographically concealed payloads, persistence mechanisms, Active Directory reconnaissance and ultimately a custom reverse WebSocket tunnel.

The most significant aspect of this campaign is **not simply malware execution on the endpoint**. The final reverse-tunneling component can transform the compromised Windows workstation into a **network pivot**, allowing an operator to establish TCP connections to systems reachable from that workstation. Microsoft reports that the tunnel uses TLS/WebSocket communication over TCP/443 and supports arbitrary TCP proxying through a SOCKS5-style address mechanism.

For organizations in Bangladesh, this presents a significant risk where employees use domain-joined Windows workstations to access:

- Active Directory;
- File servers;
- Database servers;
- Administrative systems;
- VPN infrastructure;
- Internal web applications;
- Government information systems;
- Critical-infrastructure management networks.

However, the techniques are directly applicable to Windows enterprise environments commonly deployed in Bangladesh and should therefore be treated as an immediate defensive-hunting priority.

Threat Overview

TerminalFix represents an evolution of the **ClickFix** attack technique.

Traditional ClickFix campaigns commonly manipulate users into executing commands through Windows Run or other trusted interfaces. TerminalFix adapts this technique to Windows Terminal/PowerShell, making it more suitable for executing longer and more complex command sequences.

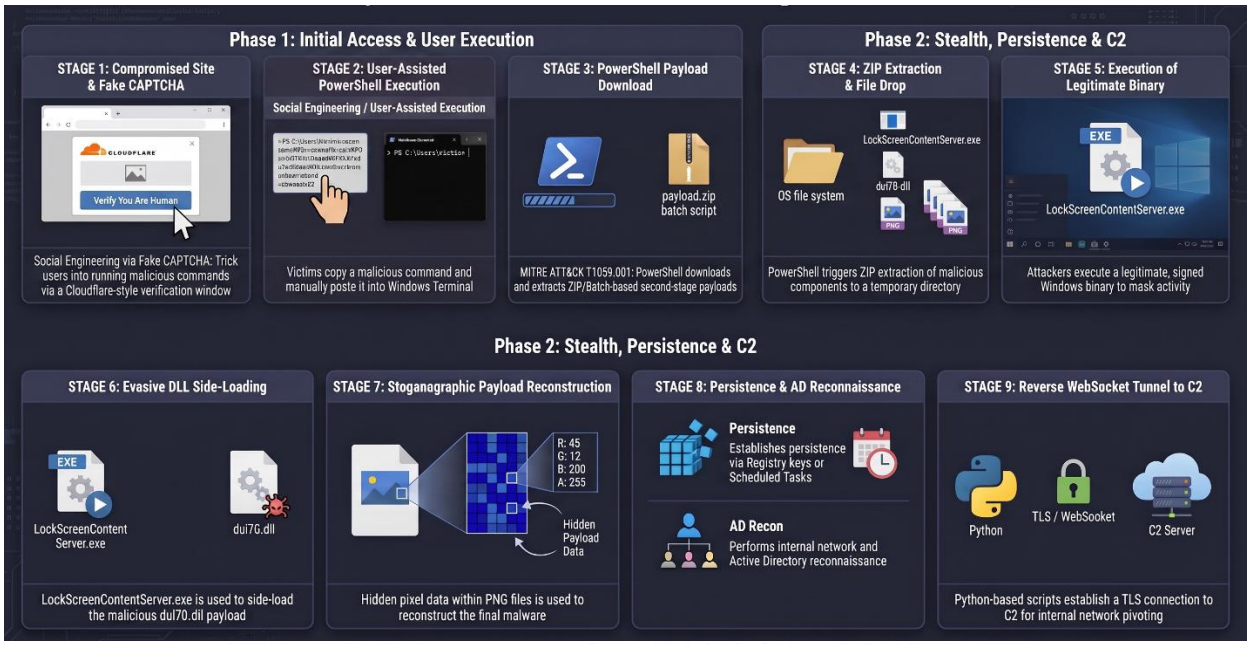


Figure: Complete TerminalFix multistage intrusion chain from ClickFix-style social engineering to reverse WebSocket tunneling and potential internal network pivoting.

BGD e-GOV CIRT

Bangladesh-Specific Risk Assessment

The campaign is particularly relevant to Bangladesh because many organizations operate Windows-based enterprise environments containing centralized Active Directory infrastructure.

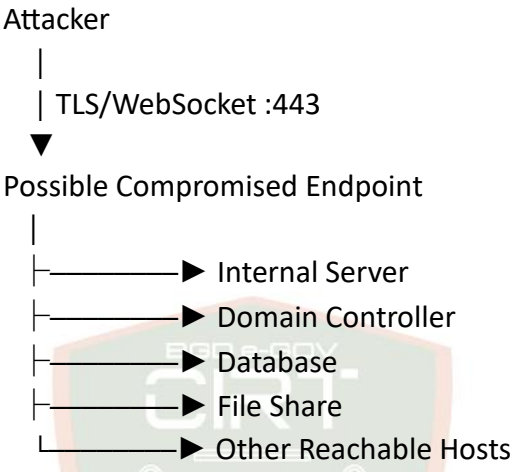
A compromised employee workstation may have network visibility to:

User Workstation

- Domain Controller
- File Server

- Database Server
- Internal Web Applications
- Management Systems
- Backup Infrastructure
- Administrative Services

If the attacker establishes a reverse tunnel on such a workstation, the external operator may not need direct Internet access to these internal systems. Instead:



This effectively turns the infected workstation into a proxy/pivot point inside the organization's trusted network. Microsoft specifically describes this capability as enabling the attacker to reach hosts visible from the compromised system.

Initial Access – Fake CAPTCHA / TerminalFix

The initial stage abuses user trust in CAPTCHA verification. The victim encounters a compromised website containing a fake Cloudflare Turnstile-style interface.
The page instructs the victim to perform a sequence resembling:

1. Verify that the user is human.
2. Copy a command.
3. Open Windows Terminal/PowerShell.
4. Paste the command.
5. Execute it.

The important distinction is that **the user performs the final execution step**. Therefore, conventional malware-download protections may not necessarily identify the initial event as malicious. Microsoft maps this behavior to:

- **T1189 – Drive-by Compromise**
- **T1059.001 – PowerShell**
- **T1204.002 – User Execution: Malicious File**

Security implication

Organizations should not train users only to avoid "downloading suspicious .exe files."

Users must also understand:
A website asking you to paste a command into PowerShell or Windows Terminal is itself a major security warning.

Figure: ClickFix-style fake CAPTCHA used to socially engineer victims into manually executing a malicious command through Windows Terminal/PowerShell

PowerShell Execution

After the victim executes the supplied command, PowerShell begins the next stage. Microsoft observed the command downloading a ZIP archive, extracting it under: `C:\ProgramData` and subsequently executing a batch file.

Detection opportunities

SOC teams should investigate:

- browser → PowerShell execution;
- PowerShell → `cmd.exe`;
- PowerShell downloading ZIP files;
- extraction into `C:\ProgramData`;
- newly created `.bat` files;
- PowerShell executing files immediately after download.

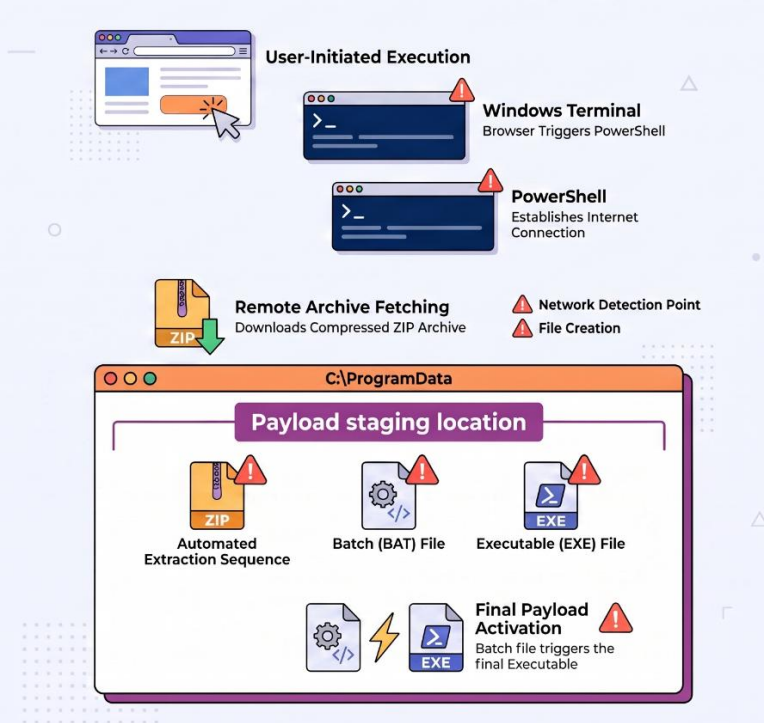


Figure: PowerShell-driven payload retrieval, extraction and staging following successful TerminalFix user execution

DLL Side-Loading

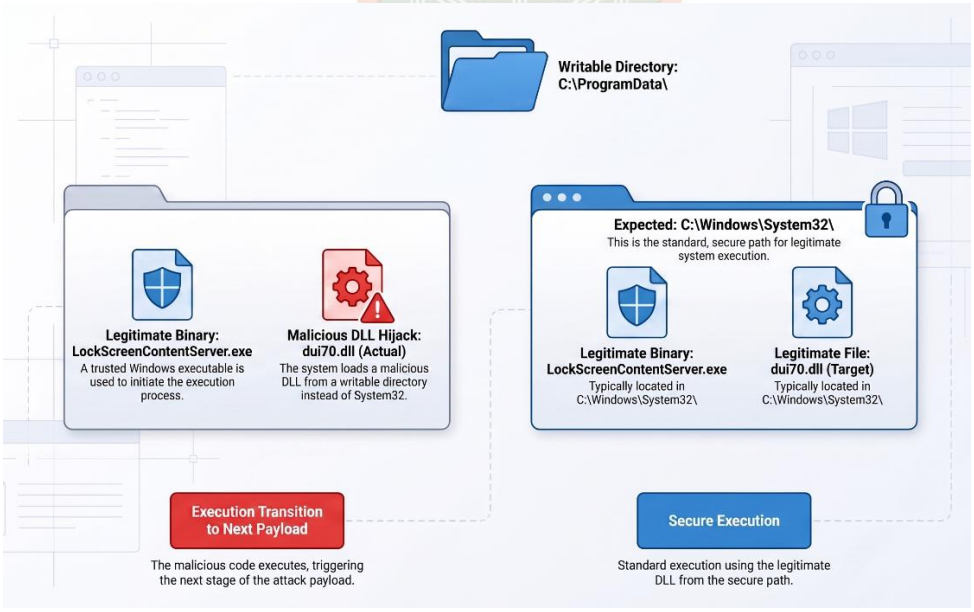


Figure: DLL side-loading in which a legitimate Windows executable is executed from an unexpected location and loads a malicious `dui70.dll`

One of the major defense-evasion techniques is DLL side-loading. The campaign uses a legitimate Windows binary:

`LockScreenContentServer.exe`

alongside a malicious: `dui70.dll`

The legitimate executable loads the malicious DLL because of Windows DLL search/order behavior. This technique abuses the trust associated with a legitimate executable rather than requiring the attacker to execute an obviously malicious executable.

Microsoft specifically recommends alerting when `LockScreenContentServer.exe` executes from locations other than its expected Windows system paths.

Steganographic Payload Delivery

The campaign adds another layer of defense evasion by hiding payload data inside PNG images.

The malicious DLL downloads PNG files and extracts data embedded within image pixel information. The recovered content is then reconstructed into executable components. This is significant because the network request may appear to retrieve an ordinary image rather than an executable.

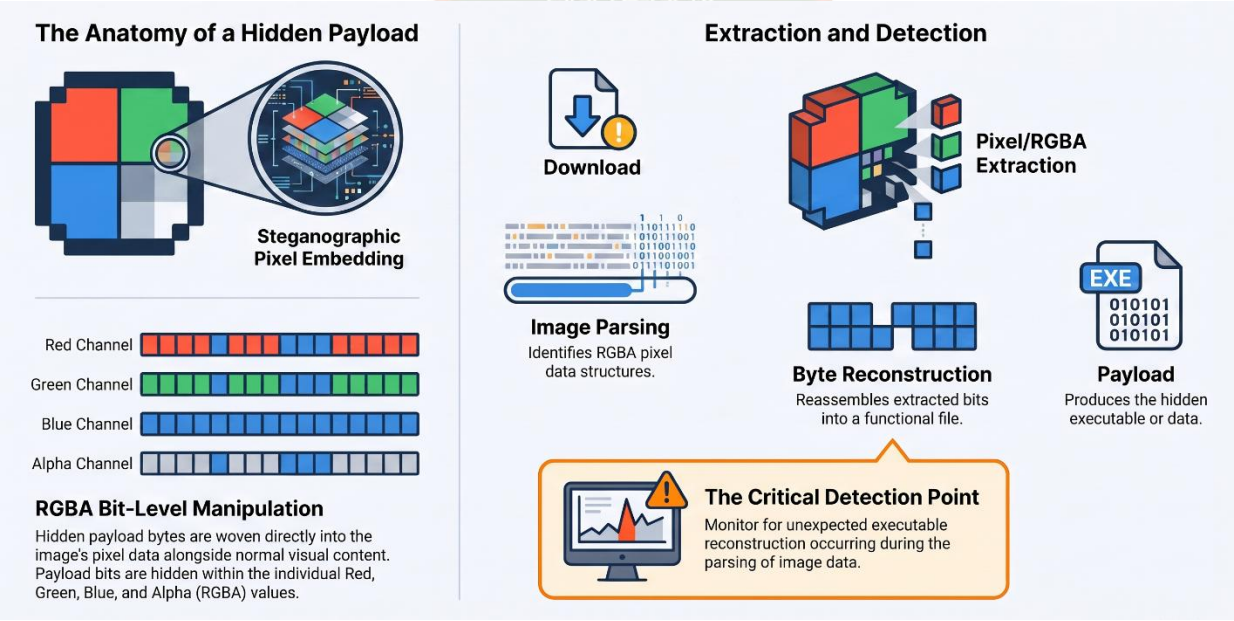


Figure: Steganographic payload delivery in which executable data is concealed within PNG image content and reconstructed at runtime

Persistence

The observed campaign establishes multiple persistence mechanisms.

Registry persistence

An HKCU Run key is used to execute the malicious executable when the user logs in.

Scheduled Task

A scheduled task executes the payload periodically, reportedly every **60 minutes.**

This redundancy increases the likelihood that access survives a simple cleanup action.

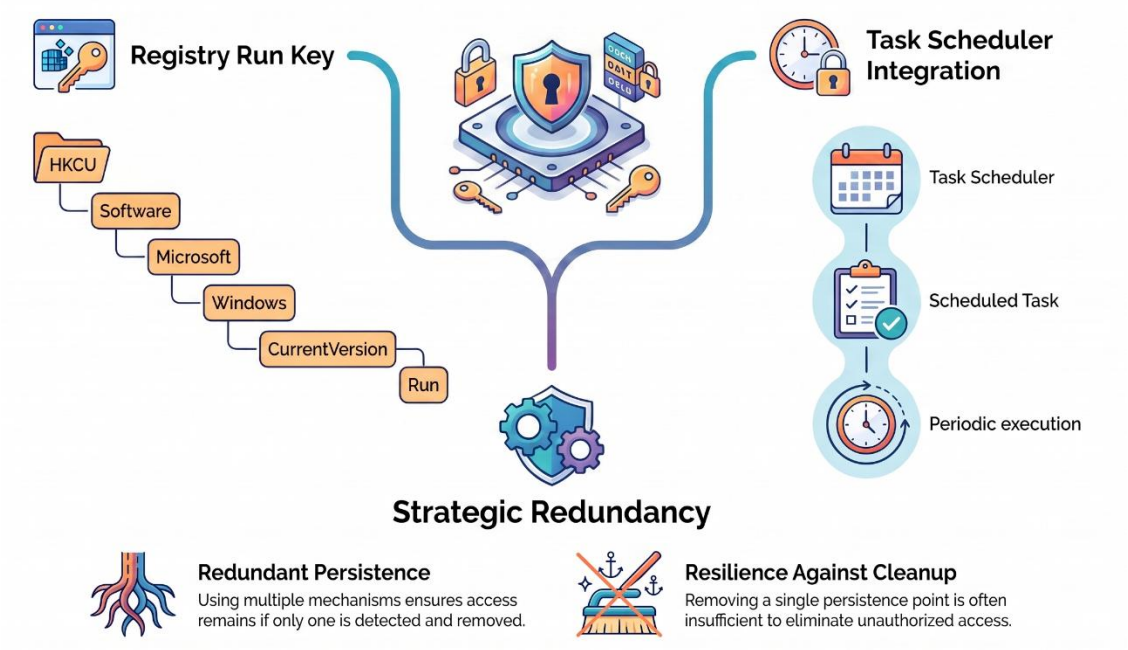


Figure: Dual persistence architecture using a user-level Registry Run key and scheduled-task execution

Hidden Files and Directories

The campaign uses Windows attributes to hide payload directories.The observed technique includes:

```
attrib +h +s
```

which applies hidden/system attributes. SOC teams should therefore include hidden directories under writable locations in endpoint hunting.

Active Directory Reconnaissance

This stage represents a major escalation in risk. The malware performs extensive reconnaissance against the organization's Windows domain.

Observed activities include:

- Domain trust discovery;
- Domain Controller discovery;
- Domain Admin enumeration;
- Domain user enumeration;
- Server discovery;
- User-description harvesting;
- System-information collection;
- Network/server ping sweeps.

Observed commands/techniques include:

- `nltest`
- `net group "domain admins" /domain`
- `ADSI Searcher`
- `systeminfo.`

This is highly valuable intelligence to an attacker preparing for lateral movement.

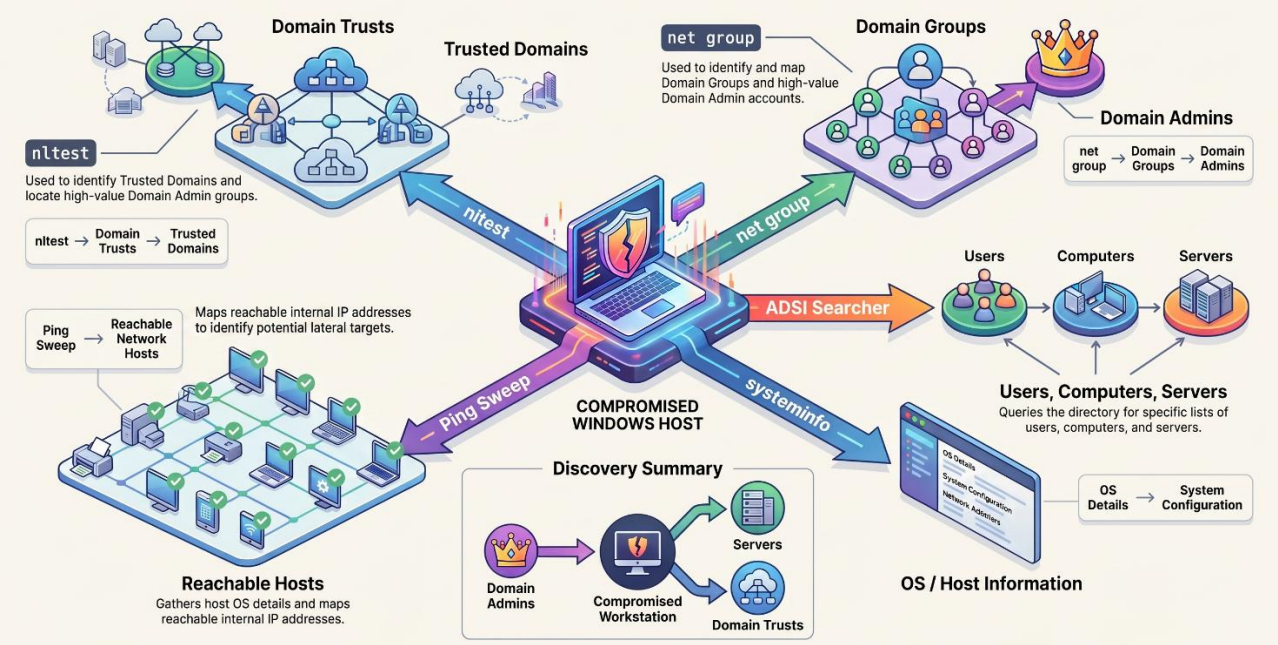


Figure: Active Directory reconnaissance performed from the compromised endpoint to identify privileged groups, domain controllers, trusts, users and reachable systems

Domain Trust Discovery

The campaign uses commands including:

- `nltest /domain_trusts`
- `nltest /dclist:`

These can reveal information about:

- domain relationships;
- domain controllers;
- Windows domain infrastructure.

Organizations should alert on these commands when executed from ordinary user workstations without an approved administrative or troubleshooting reason.

Domain Admin Discovery

The campaign reportedly executes:

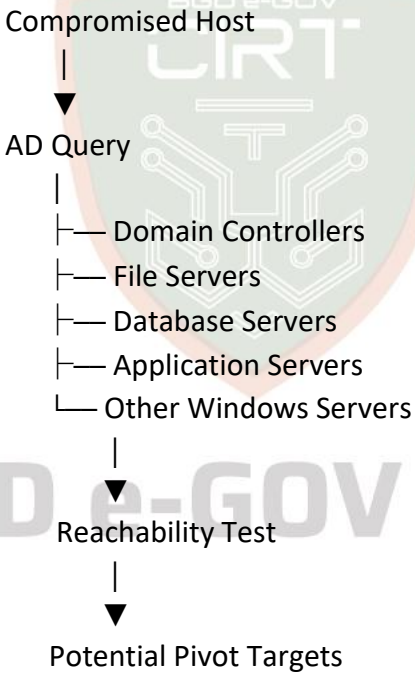
```
net group "domain admins" /domain
```

This is particularly important because enumeration of privileged groups from a compromised employee workstation may indicate preparation for privilege escalation.

Remote System Discovery

The malware uses Active Directory queries to identify Windows Server systems and performs targeted ping sweeps.

This can produce an internal target map:



BGD e-GOV CIRT

Command Execution Loop

Another component creates an asynchronous command-execution mechanism by monitoring a text file for new commands.

This provides a simple mechanism for remote command execution without requiring the attacker to maintain an interactive shell.

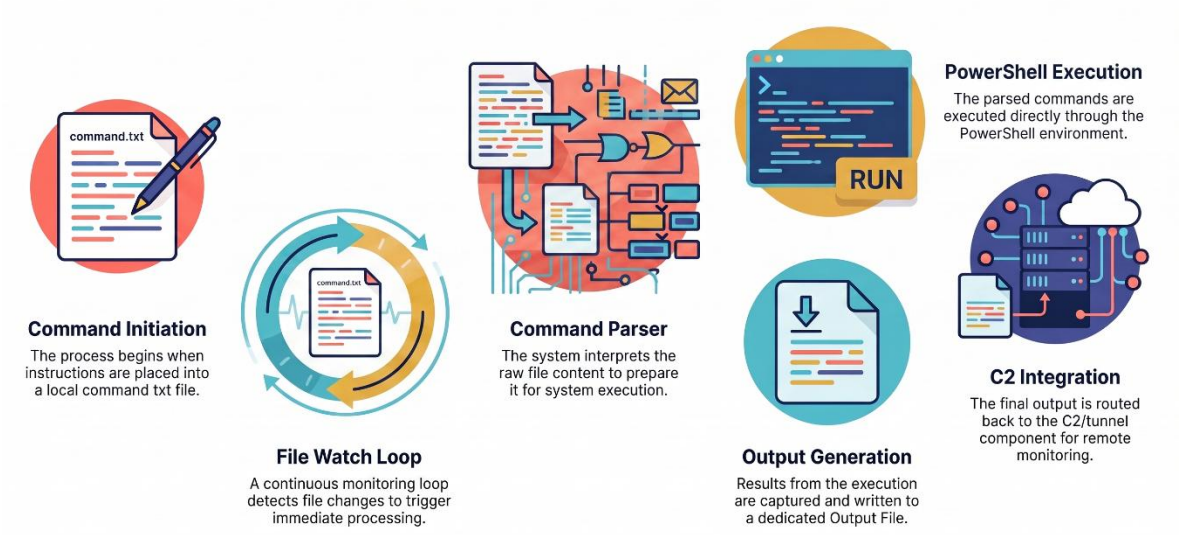


Figure: File-based command execution mechanism used to process externally supplied commands and return execution output

Reverse Tunnel

The final stage is the most important technical capability. The campaign downloads an embeddable Python runtime and launches:

`pythonw.exe`

with the custom:

`client.py`

tunneling component. The Python runtime observed by Microsoft was version **3.14.5** and was downloaded from the official Python distribution infrastructure.

BGD e-GOV CIRT

Reverse WebSocket Tunnel

The implant establishes an outbound TLS connection to: `gitnow[.]dev:443` and upgrades the connection to WebSocket.

The tunnel supports:

- arbitrary TCP connections;
- SOCKS5-style address parsing;
- IPv4;
- IPv6;
- hostnames;
- multiplexed streams;
- remote shutdown;
- persistent communication.

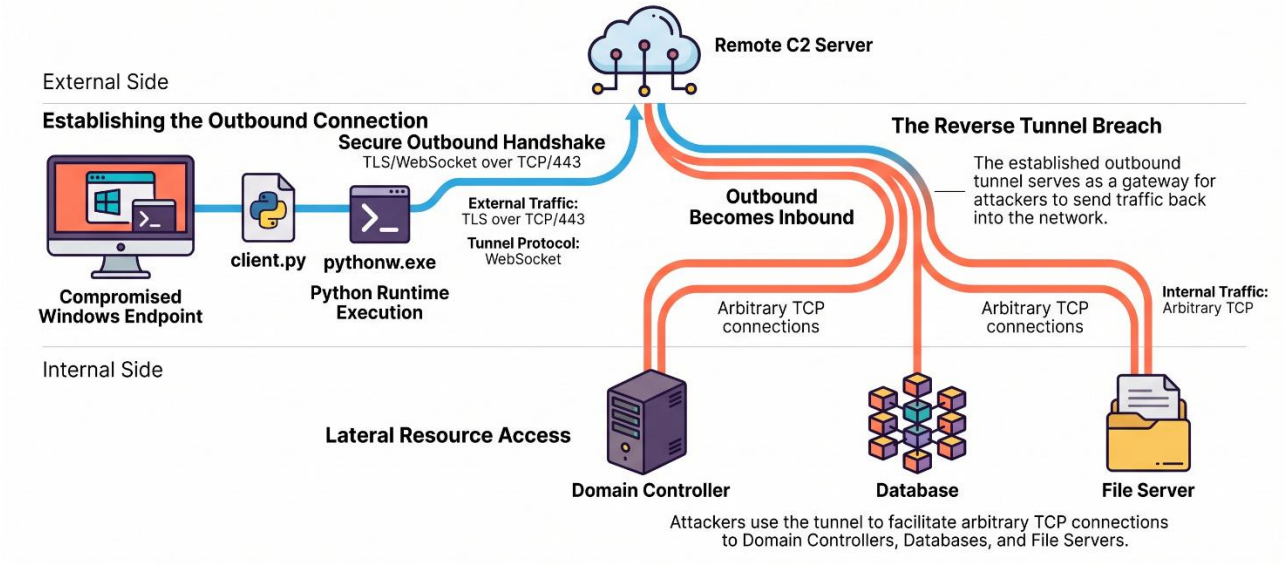


Figure: Reverse WebSocket tunnel allowing the compromised endpoint to act as a potential network pivot toward internally reachable systems

Why Reverse Tunneling Is Dangerous

Normally `Internet → Internal Server` is blocked by perimeter firewalls.
With a reverse tunnel:

Internal Host
|
| outbound HTTPS/WebSocket
▼
Attacker
|
▼
Tunnel
|
▼
Internal Target

The attacker can therefore potentially use an already-compromised endpoint as a **bridge into the organization's internal network**.

Microsoft specifically states that the implant's arbitrary TCP capability can reach hosts visible from the compromised system. The observed capability should not, by itself, be interpreted as evidence that specific internal systems were successfully compromised. Rather, it represents an enabling capability that could facilitate subsequent reconnaissance, credential attacks, lateral movement, or access to internal services. The source analysis explicitly notes that downstream actions were not observed in the analyzed chain.

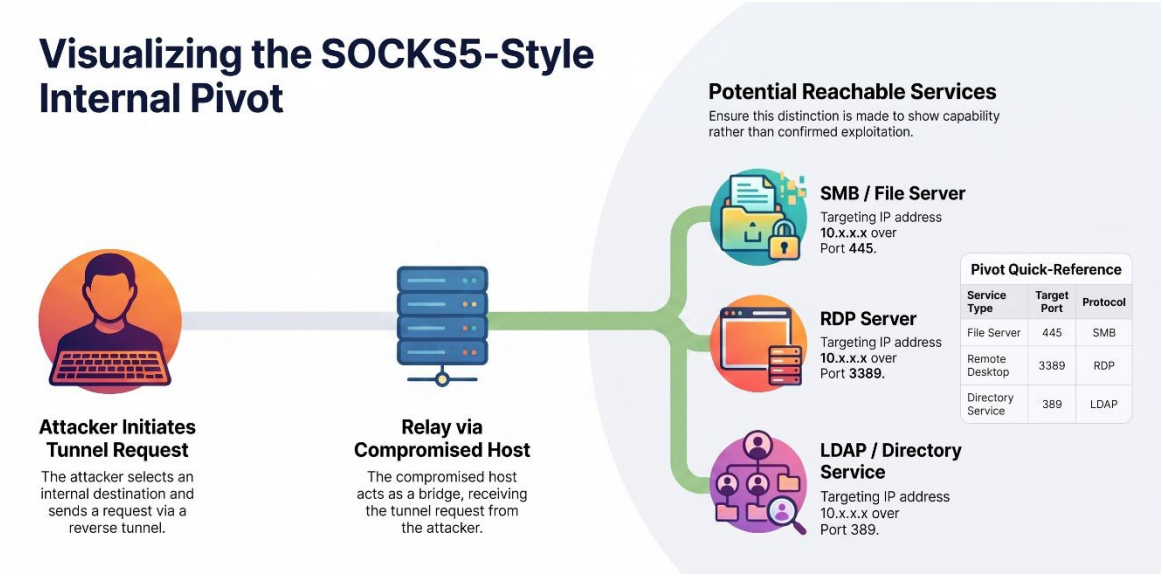


Figure: Conceptual representation of arbitrary TCP forwarding through the reverse tunnel, enabling potential access to services reachable from the compromised endpoint

Attack to Impact Scenario

A plausible enterprise attack path would be:

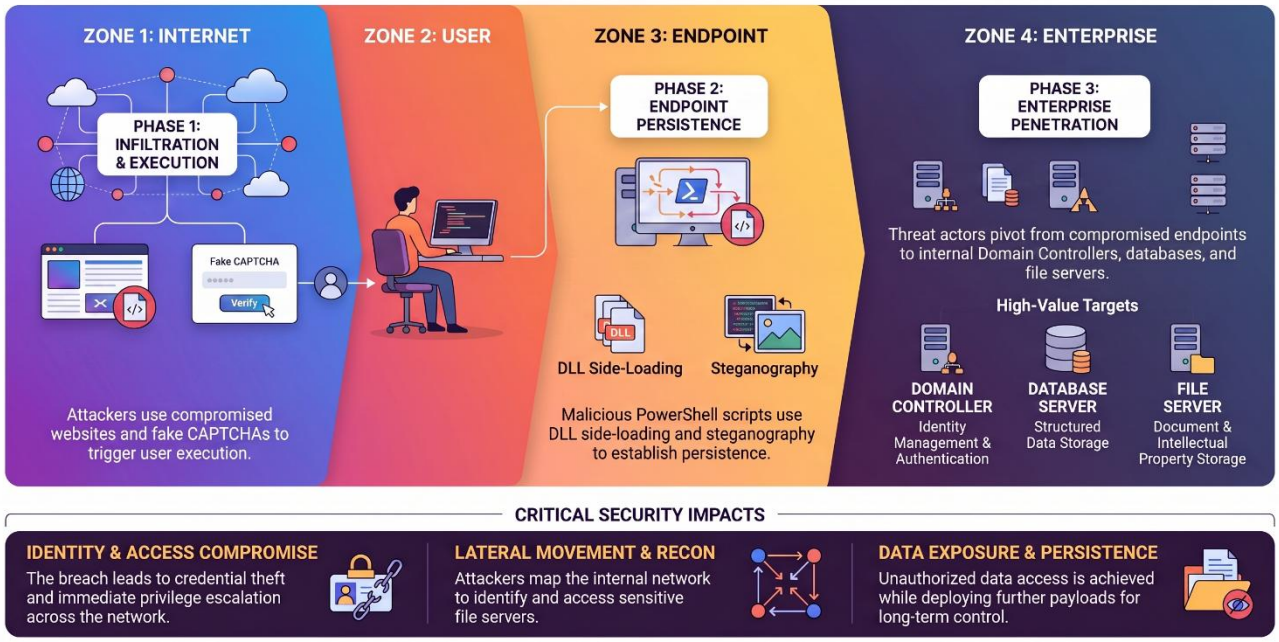


Figure: End-to-end TerminalFix intrusion architecture showing progression from social engineering to endpoint compromise, Active Directory reconnaissance and potential internal network access

This scenario is particularly relevant for government agencies, financial institutions, telecommunications operators, universities, healthcare organizations and critical infrastructure operators using centralized Windows/AD environments.

MITRE ATT&CK Mapping

Tactic	Technique	ID
Initial Access	Drive-by Compromise	**T1189**
Execution	PowerShell	**T1059.001**
Execution	User Execution	**T1204.002**
Persistence	Registry Run Keys	**T1547.001**
Persistence	Scheduled Task	**T1053.005**
Defense Evasion	DLL Side-Loading	**T1574.002**
Defense Evasion	Steganography	**T1027.003**
Defense Evasion	Hidden Files/Directories	**T1564.001**
Defense Evasion	Masquerading	**T1036.005**
Discovery	Remote System Discovery	**T1018**
Discovery	Domain Group Discovery	**T1069.002**
Discovery	Domain Trust Discovery	**T1482**
Discovery	Domain Account Discovery	**T1087.002**
Discovery	System Information Discovery	**T1082**
C2	Protocol Tunneling	**T1572**
C2	Web Protocols	**T1071.001**
Command/Transfer	Ingress Tool Transfer	**T1105**

Indicators of Compromise (IoC)

Network Indicators

Indicator	Type	Purpose
`gitnow[.]dev`	Domain	**Reverse-tunnel C2, TCP/443**
`bestsocialmedianewspapper[.]com`	Domain	**Steganographic payload hosting**
`offlineupdater[.]com`	Domain	**Payload hosting/failover**
`linked-log[.]com`	Domain	**Compromised website**

File Hashes

SHA-256	Description
18c2090e8a0ae0568af9b87e59eaf8270f23d2909600ed9db91a9444fd8b278f	verify_pkg.zip
b8d107800403b9197e5b7609ceacd8e4cac1b0f9a1d156e6dacd6c3f7794b36a	client.py
ba77feed86bcda49308746421bdc684a432dd5d68c363975b2a3c6831bda3f07	dui70.dll
026478003fe35413403acf6890e7d3b153ba08a836eca42350db48f213872ab	dui70.dll
032b529fac61e550f5dc9489686f519b82d64625fa05a8d9ecf8ba8be9b2ad22	dui70.dll
df8221a933b38284ebdcb8bffc2df62123c9f5b5f421dd0b070e13e668b3eabf	dui70.dll
eb1b4be34d05b394fb74efdeb95faecd1d1963be6ecc1b9db2b4757b491f01f0	dui70.dll
5d43abf5c36ea203176d3300ff14af27b4be81810ad2679b3a62b255e3d6e1c8	dui70.dll
9a7b4dcd51d9251c177d323d6aaecdfc86674f69bc1af048dc872926d22aaa24	dui70.dll
342df92235c9dec81203b837addaa38bb85b64b4a48fe71b5303ca86d991991e	dui70.dll
ededeacf30e493dd632d477fe770ba419aa2848f685ea049381a0a8d2cc3e84d	dui70.dll

BGD e-GOV CIRT

Detection and Monitoring

Endpoint Monitoring

Monitor for:

- Browser → PowerShell execution;
- PowerShell → `cmd.exe`;
- ZIP extraction into `C:\ProgramData`;
- `LockScreenContentServer.exe` executing outside expected directories;
- `dui70.dll` loaded by that executable;
- `python.exe / pythonw.exe` launched from unusual locations;
- `client.py`;
- `attrib +h +s`;
- new scheduled tasks;
- new HKCU Run keys.

Active Directory Monitoring

Alert on unexpected execution of:

- `nltest`
- `net group`
- `systeminfo`
- `ADSI queries.`

Especially when these occur shortly after:

```
PowerShell execution
+
new persistence
+
external network connection
```

This combination is significantly more suspicious than any single event alone.

Network Monitoring

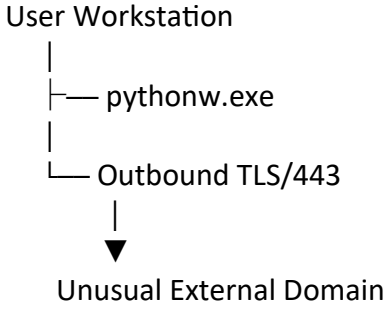
Monitor outbound:

- TLS/443
- WebSocket upgrades

Especially when initiated by:

- `python.exe`
- `pythonw.exe`
- `powershell.exe`
- `cmd.exe`
- `LockScreenContentServer.exe`

A key detection opportunity is:



Port 443 alone should **not** be treated as malicious; the process, destination, timing and behavioral context are critical.

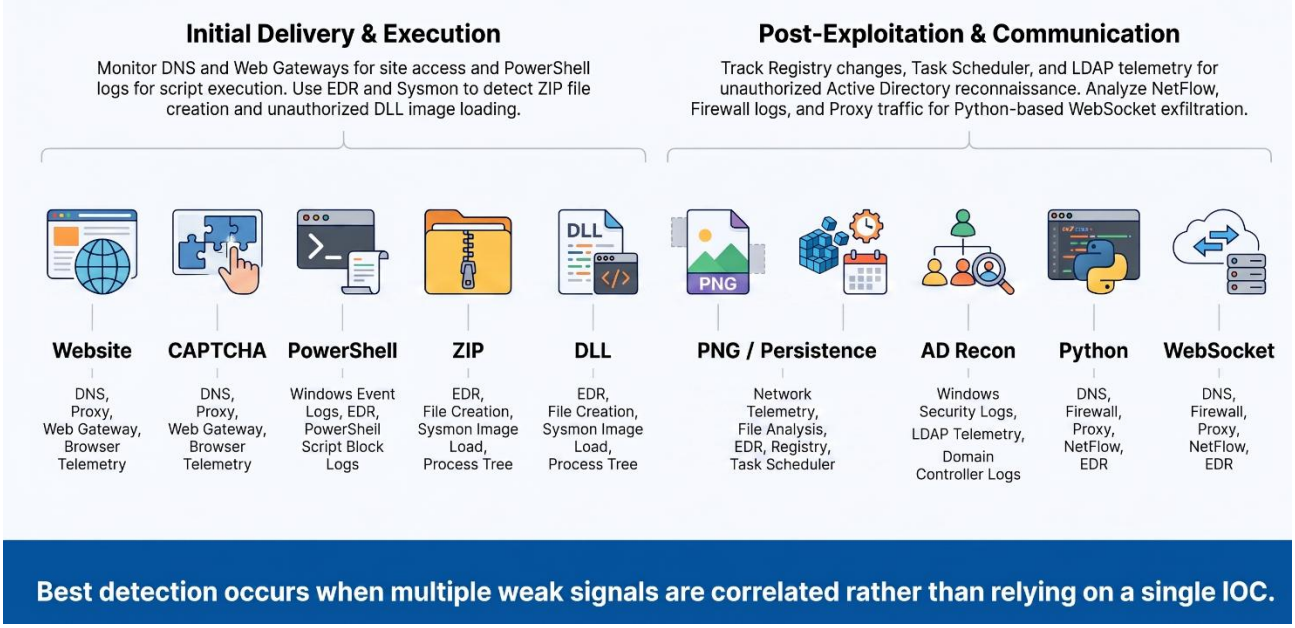


Figure: Detection telemetry mapped to individual stages of the TerminalFix attack chain, highlighting opportunities for endpoint, network, identity and SIEM correlation

Recommended Actions

- Educate users that legitimate CAPTCHA systems do not require users to paste commands into PowerShell or Windows Terminal.
- Restrict unnecessary PowerShell access for standard users.
- Monitor browser-to-PowerShell process chains.
- Detect LockScreenContentServer.exe executing from non-standard directories.
- Hunt for dui70.dll.
- Hunt for the listed network indicators.
- Investigate unexpected Python/PythonW execution.
- Review newly created scheduled tasks and HKCU Run keys.

Microsoft recommends PowerShell restrictions, application control, monitoring DLL side-loading, user awareness against ClickFix-style tactics, and thorough investigation of affected hosts.

Incident Response Guidance

If any of the high-confidence indicators are identified.

Isolate

Immediately isolate the endpoint from:

- Internet;
- corporate LAN;

- VPN;
- privileged administrative networks.

Preserve Evidence

Before remediation, collect:

- memory;
- PowerShell logs;
- process tree;
- scheduled-task definitions;
- Registry Run keys;
- DNS logs;
- proxy logs;
- firewall logs;
- network connections;
- suspicious PNG files;
- ZIP archives;
- DLLs;
- Python runtime;
- `client.py`

Assume Network Exposure

Because the reverse tunnel provides potential internal TCP access, the compromised endpoint should not be treated as an isolated malware infection. Microsoft recommends credential rotation for credentials accessible from an affected machine, including domain-administrator credentials where the host is domain joined.

Investigate:

1. Endpoint
2. Internal connections
3. Authentication
4. AD queries
5. Administrative activity
6. Data access

Credential Investigation

If a domain-joined endpoint is compromised, investigate whether the attacker accessed:

- cached credentials;
- browser credentials;
- authentication tokens;

BGD e-GOV CIRT

- password managers;
- SSH keys;
- service credentials;
- privileged credentials;
- administrative sessions.

Priority should be given to credentials belonging to:

- Domain Administrators;
- server administrators;
- network administrators;
- database administrators;
- security administrators.

The TerminalFix campaign demonstrates a significant evolution in social-engineering-led intrusion. For Bangladesh, BGD e-GOV CIRT therefore assesses this activity as a HIGH enterprise threat, particularly for organizations with:

- large Windows/Active Directory environments;
- privileged users operating from standard workstations;
- weak PowerShell restrictions;
- limited east-west network monitoring;
- unrestricted outbound HTTPS;
- insufficient network segmentation.

There is no evidence in the referenced Microsoft report establishing that Bangladesh has been specifically targeted or compromised by TerminalFix. Accordingly, this advisory should be used as a proactive threat-hunting and defensive-preparedness advisory for Bangladesh, rather than as confirmation of a Bangladesh-specific incident.

BGD e-GOV CIRT

References

- https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/
- https://www.darkreading.com/threat-intelligence/terminalfix-campaign-weaponizes-powershell-enterprise-attacks

BGD e-GOV CIRT