ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR



FaCai APT: Targeted Phishing Campaign Leveraging DLL Side-Loading and Vulnerable Drivers

TLP: CLEAR
Distribution: Public
Advisory on: FaCai APT: Targeted Phishing Campaign Leveraging DLL Side-Loading and Vulnerable Drivers
Severity: High
Threat Category: Cyber Espionage / Malware Delivery / Defense Evasion
Threat Actor: FaCai activity cluster (overlap with Silver Fox)
Geographic Scope: Europe, Asia and Middle East & Africa (MEA)
Date: 19 November 2026

Executive Summary

BGD e-GOV CIRT has identified intelligence concerning an ongoing targeted phishing campaign attributed to a newly tracked threat activity cluster known as **FaCai**, which exhibits significant operational overlap with the previously reported Silver Fox activity cluster.

The campaign primarily relies on spear-phishing emails containing malicious attachments packaged in formats such as Virtual Hard Disk (VHD), disk image (IMG), and ZIP archives. These files contain a legitimate, digitally signed executable alongside a malicious Dynamic Link Library (DLL). When a victim executes the legitimate application, the malicious DLL is loaded through a technique known as **DLL side-loading**, initiating the infection chain.

The initial DLL functions as a downloader and exhibits configuration characteristics associated with Valley RAT. It communicates with hardcoded Command and Control (C2) infrastructure to retrieve additional payloads, including shellcode and a Core RAT component.

A particularly concerning feature of this campaign is its use of vulnerable kernel drivers to terminate protected antivirus and Endpoint Detection and Response (EDR) processes. The analyzed activity includes the malicious deployment of an OPSWAT AppRemover kernel driver associated with **CVE-2026-36425**, an improper access control vulnerability that reportedly enables an unprivileged local user to issue process termination requests through the affected driver.

The malware also incorporates an execution-expiration mechanism. Its primary malicious functionality is suppressed when the sample is executed after a configured expiration date, at which point it displays a warning message instead.

Although the supplied intelligence does not establish confirmed compromise of Bangladeshi organizations, the campaign's phishing-based delivery, security-product evasion techniques, and RAT deployment capabilities present a potential risk to government institutions, financial organizations, telecommunications providers, and other critical sectors in Bangladesh.

Organizations are advised to strengthen email security, inspect suspicious attachments, monitor DLL side-loading activity, protect endpoint security processes, and investigate the associated indicators.

Threat Overview

Threat Actor Profile

FaCai is a newly tracked activity cluster identified by Group-IB Threat Intelligence. The observed campaign demonstrates significant overlap with Silver Fox, particularly in its use of Valley RAT-style components and associated configuration structures.

The activity involves targeted spear-phishing, malicious DLL loading, deployment of additional payloads, and attempts to disable endpoint security controls.

The attribution should be treated as an activity-cluster assessment rather than definitive proof that FaCai and Silver Fox are the same threat actor.

Campaign Characteristics

Attribute	Observed characteristics
Initial access	Targeted spear-phishing emails
Delivery mechanism	Malicious attachments
Container formats	VHD, IMG and ZIP
Execution technique	DLL side-loading
Initial malware	DLL downloader / Valley RAT-style login module
Subsequent payload	Shellcode and Core RAT
Defence evasion	Vulnerable kernel-driver deployment
Security products targeted	Multiple antivirus and EDR solutions
C2 communication	Hardcoded domains and configured ports
Execution control	Configured campaign expiration date
Threat attribution	FaCai activity cluster; overlap with Silver Fox

BGD e-GOV CIRT

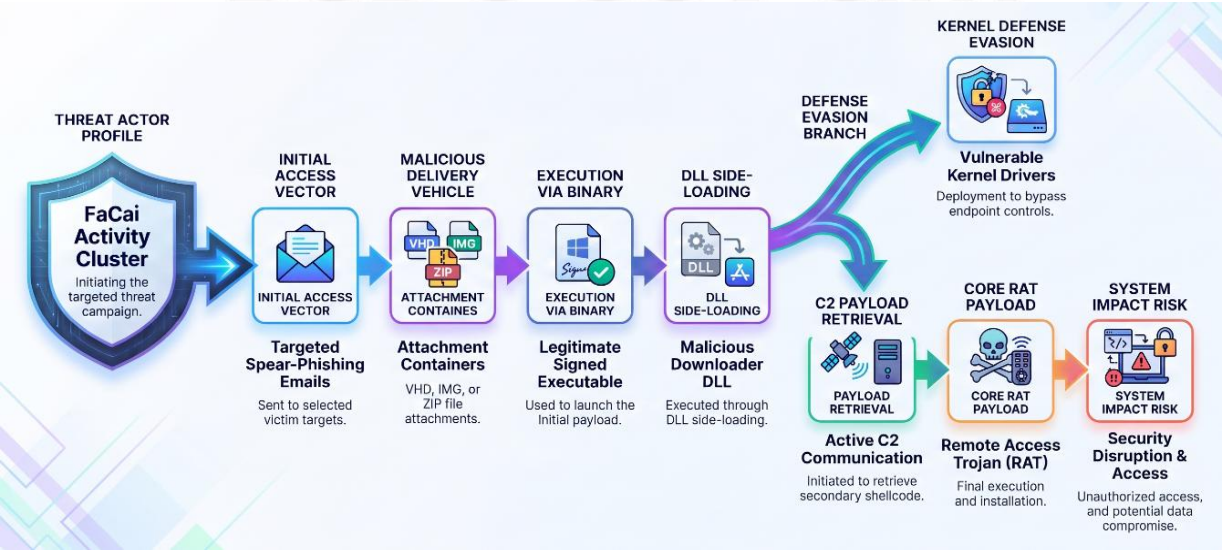


Figure: High-level overview of the FaCai phishing and malware deployment chain

Technical Analysis

Initial Access: Targeted Spear-Phishing

The campaign begins with targeted spear-phishing emails containing malicious compound files. The social-engineering themes observed in the emails suggest that the threat actors may possess prior knowledge of the targeted organizations and their operational environments.

The attachments contain a legitimate, digitally signed executable and a malicious DLL. The legitimate executable is used as the execution mechanism for loading the malicious DLL.

The campaign has been observed using the following container formats:

- Virtual Hard Disk (VHD)
- Disk Image (IMG)
- ZIP archive

The use of legitimate signed applications may make the initial execution appear less suspicious to users and, in some circumstances, security monitoring systems.

DLL Side-loading and Initial Payload Execution

After the victim extracts and executes the legitimate application, the application loads the malicious DLL from its execution directory.

The DLL acts as a downloader and contains a configuration structure associated with Valley RAT-style functionality. Analysis indicates that nearly all exported functions in the observed DLL are virtualized, apparently using VMProtect. Other functions remain unobfuscated but lack direct cross-references, suggesting that virtualized routines may dynamically resolve and invoke them.

Before proceeding, the DLL checks for an existing instance through a mutex. If the mutex is not present, it enables several operational privileges:

- `SeDebugPrivilege`
- `SeLoadDriverPrivilege`
- `SeIncreaseBasePriorityPrivilege`
- `SeTakeOwnershipPrivilege`

The DLL subsequently copies itself and the legitimate executable into a randomly generated directory under: `C:\ProgramData`

Execution then restarts from the newly created directory.

Vulnerable Driver Deployment and Security Evasion

One of the most significant characteristics of this campaign is the use of vulnerable kernel drivers to terminate protected antivirus and EDR processes.

Before deploying the final payload, the loader retrieves one of three encrypted vulnerable drivers embedded in its resource section. Driver selection depends on a key string passed to the driver-loading routine.

The selected driver is decrypted using RC4 with a dynamically generated 16-byte key.

The observed driver resources include:

Key string	Resource identifier	Vulnerable driver
Marquee	`0x43C`	OPSWAT AppRemover (`ardrv.sys`)
MaterialIcons	`0x43D`	ZyArk `(ZYArKit.sys)`
Mobile	`0x43E`	`Alinubx.sys`

The recovered RC4 key is: `88042CFF2F4810520D31E711973A5BFA`

The analyzed campaign specifically used an OPSWAT AppRemover kernel driver associated with **CVE-2026-36425**. The reported improper access control vulnerability allows an unprivileged local user to open the affected device object and issue process termination requests.

This capability can be abused to terminate protected security processes, weakening endpoint protection before the subsequent malware payload is deployed.
The malware contains an extensive list of process names associated with multiple antivirus and EDR products, including Microsoft Defender, McAfee, Kaspersky, Avast, AVG, Norton, Trend Micro, Sophos, CrowdStrike, SentinelOne, Cylance, Carbon Black, Fortinet and AhnLab. The process-name lists are hex-encoded and RC4-encrypted within the binary. Their intended purpose appears to be runtime identification of security products, although the supplied analysis could not conclusively establish whether all listed process checks are executed.

C2 Communication and Payload Retrieval

Following driver deployment and completion of its preliminary checks, the DLL establishes communication with hardcoded C2 infrastructure. The recovered configuration contains the following C2 domain and ports:

C2 domain	Port	Configuration field
`fluxorv[.]top`	443	A1 / o1
`fluxorv[.]top`	80	S2 / o2
`fluxorv[.]top`	9999	p3 / o3

The configuration also contains the following mutex: `3F0CBB671BEEBBA0BD9`

The configuration fields define the C2 server hostnames and associated ports, with priority and transport-related flags. The analyzed sample retrieves a C2 package containing a shellcode blob and a primary RAT executable. The payload is subsequently stored and executed through registry-based staging and in-memory execution.

The following registry locations were identified:

- `HKEY_CURRENT_USER\Console\0`
- `HKEY_LOCAL_MACHINE\SOFTWARE\IpDates_i4`

The first location is associated with storage of subsequent payload modules, while the second is used to store the patched configuration.

Finally, execution is transferred to shellcode in memory, which loads and executes the downloaded module.

Time-Based Execution and Expiration Mechanism

The campaign incorporates a configuration-based execution-expiration mechanism.

The analyzed sample contained the following configuration timestamp: 2026-11-11

The malware appears to evaluate this date during execution. If the sample is executed after its configured expiration threshold, it suppresses its primary malicious functionality and displays a Chinese-language warning message:

The program has been expired for over a day. To avoid disrupting your use, please renew as soon as possible.



Figure: Time-Based Execution and Expiration Mechanism (Group-IB)

This behaviour may complicate retrospective malware analysis because the sample may not execute its malicious functionality when examined after the configured expiration date.

The expiration mechanism should not be interpreted as evidence that the associated C2 infrastructure or other campaign samples are inactive.

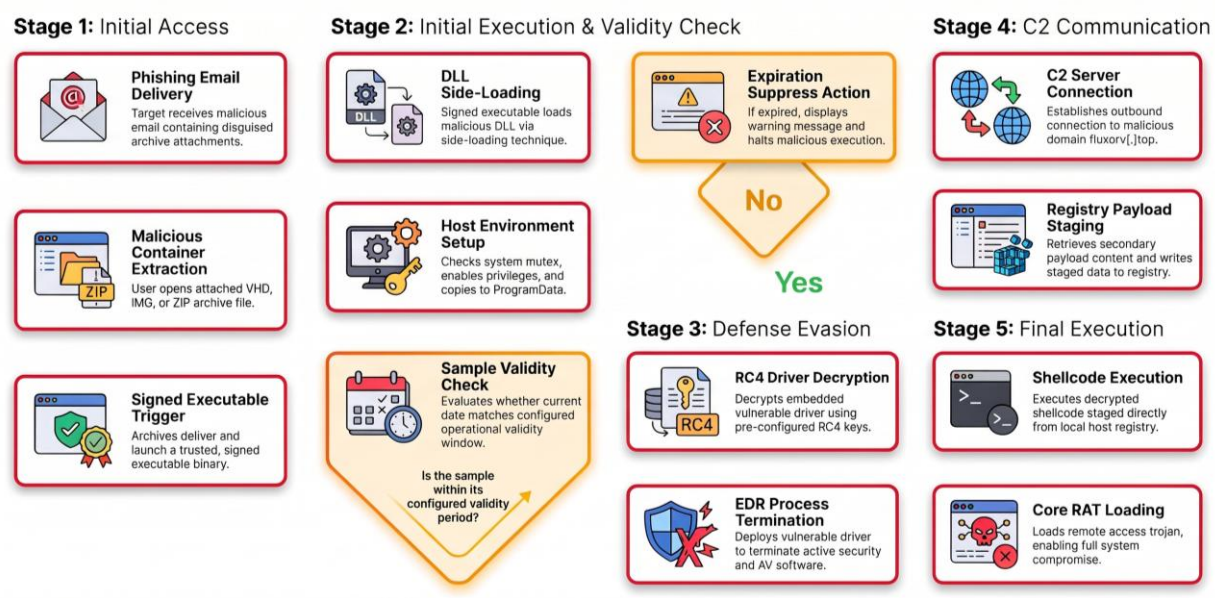


Figure: Technical execution sequence observed in the FaCai phishing campaign.

Indicators of Compromise (IoCs)

The following indicators were identified in the supplied threat intelligence. Organizations should use them for threat hunting and detection while validating any matches against additional telemetry.

Network Indicators

Indicator type	Indicator	Description
C2 domain	fluxorv[.]top	Observed C2 infrastructure
C2 port	TCP/UDP configuration on port 443	C2 configuration entry
C2 port	TCP/UDP configuration on port 80	C2 configuration entry
C2 port	TCP/UDP configuration on port 9999	C2 configuration entry

Note: The supplied configuration contains transport flags, but the exact transport protocol for each connection should be validated before creating protocol-specific blocking rules.

Host-Based Indicators

Indicator type	Indicator
Mutex	`3F0CBB671BEEBBA0BD9`
Registry path	`HKEY_CURRENT_USER\Console\0`
Registry path	`HKEY_LOCAL_MACHINE\SOFTWARE\IpDates_i4`
File location	Randomly generated directory under C:\ProgramData
Driver	`ardrv.sys`
Driver	`ZYArKit.sys`
Driver	`Alinubx.sys`
RC4 key	`88042CFF2F4810520D31E711973A5BFA`

Additional Mutex Indicator

The supplied analysis also identifies the following long hexadecimal value under the mutex indicators:

```
F3ADEDDDE6957081843C639CF3053B7D57B379D8C979F6A290CABDC465FE31B0DE57
5D61CBBB60C5846A9CBD3E8D2E25304EA914DB7DCF2423FF9D6FD2C11C357C32E4BE
9438B58793E01FFCFA6869D88A69250218B0526DE9CB0CE9D5788BA9F3825041753C
9F706AFC24135FF1FCFC63F856153BB49D77FC538D6CAE8514468C69BACEADB80964
15C89E19A5580491A69877BEB092E8422F61B36CCD7A3FAF9C5CB480480C0DE66FAB
C11D496F7558E40C1691896D9A93F4B588B4B9D8EA4AF56149C6
```

Its precise runtime role should be validated before using it as a standalone detection indicator.

Detection Considerations

Security teams should monitor for:

- Suspicious signed executables loading DLLs from the same extracted archive or writable directories.
- Newly created or randomly named directories under `C:\ProgramData`.
- Unexpected loading of kernel drivers, particularly from unusual or temporary directories.
- Attempts to load `ardrv.sys`, `ZYArKit.sys`, or `Alinubx.sys` outside legitimate software maintenance activity.
- Unexpected termination of antivirus or EDR processes.
- Suspicious access to the identified registry paths.
- Outbound connections to `fluxorv[.]top` and associated ports.
- Execution of shellcode or PE payloads from memory.
- Unusual changes to endpoint security service states.

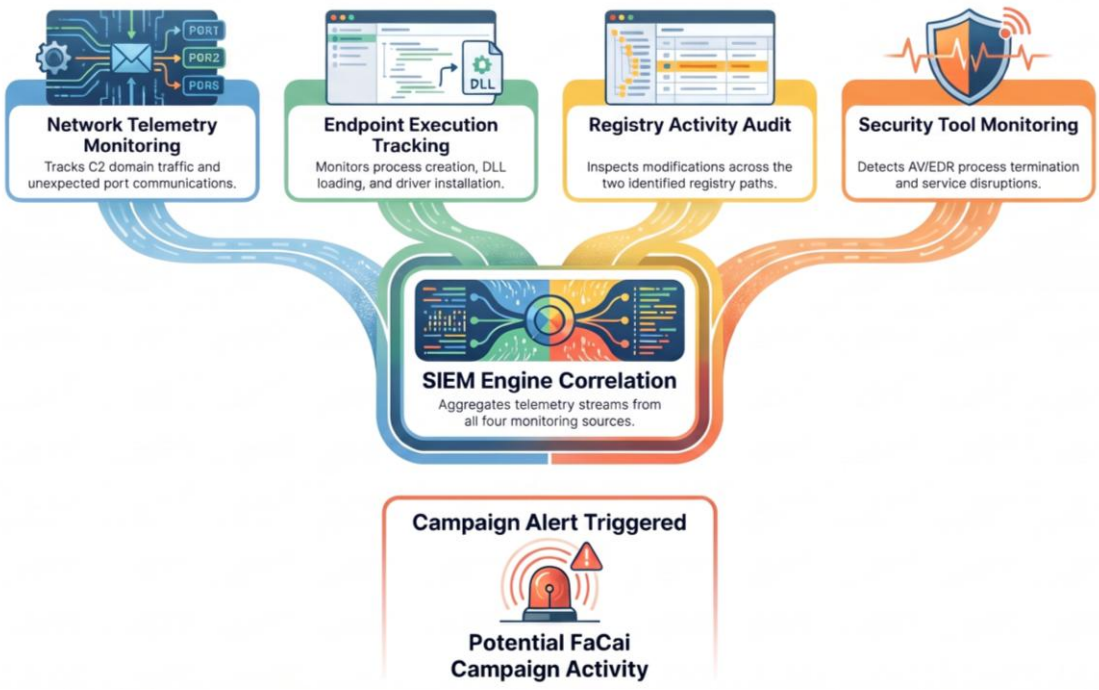


Figure: Recommended host-based and network-based detection points for the FaCai campaign.

Potential Impact

Successful execution of this campaign may result in:

- Unauthorized access to compromised systems.
- Deployment of a remote access Trojan.
- Remote command execution and control of infected endpoints.
- Disruption or termination of antivirus and EDR processes.
- Reduced visibility for endpoint security monitoring.
- Collection or potential exfiltration of sensitive organizational information.
- Further malware deployment and lateral movement, depending on the capabilities of the delivered RAT and the attacker's objectives.

The deployment of vulnerable kernel drivers is particularly concerning because it can undermine endpoint protection and make subsequent malicious activity more difficult to detect.

Relevance and Potential Exposure in Bangladesh

The campaign's use of spear-phishing and legitimate signed executables makes it relevant to organizations operating government, financial, telecommunications, energy, healthcare and other critical information systems in Bangladesh.

Potentially exposed environments include:

- Government ministries, departments and agencies.
- Critical Information Infrastructure (CII) organizations.
- Financial institutions and banking networks.
- Telecommunications and internet service providers.
- Healthcare and educational institutions.
- Organizations using Windows-based endpoints with centrally managed antivirus and EDR solutions.

The availability of the malicious attachment formats and the use of trusted-looking executables may increase the likelihood of successful initial execution where email filtering, application control and user awareness measures are insufficient.

At the time of preparing this advisory, the supplied intelligence does not establish confirmed exploitation or compromise of specific Bangladeshi organizations. The above assessment reflects potential exposure based on the observed campaign techniques.

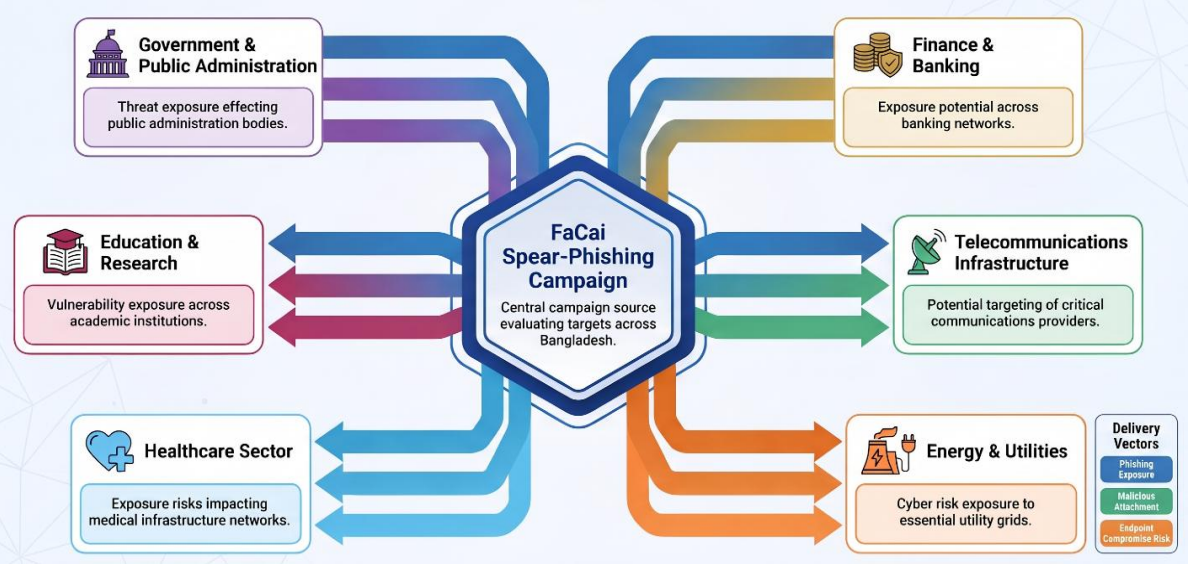


Figure: Potential exposure of key sectors in Bangladesh to the FaCai phishing campaign.

Recommendations and Mitigation Measures

BGD e-GOV CIRT recommends that organizations implement the following measures:

Email Security and Phishing Prevention

- Strengthen email gateway filtering to identify suspicious attachments and phishing messages.
- Apply additional scrutiny to VHD, IMG and ZIP attachments received from external sources.
- Block or quarantine suspicious attachments according to organizational risk policies.
- Use sandbox analysis to inspect suspicious executable and DLL combinations.
- Implement SPF, DKIM and DMARC to reduce email spoofing risks.
- Conduct targeted awareness sessions for employees, particularly users with privileged access.

Endpoint Protection and Application Control

- Ensure antivirus and EDR solutions are updated and operating normally.
- Enable tamper protection and restrict unauthorized termination of security processes.
- Implement application allowlisting and restrict execution from user-writable directories.
- Monitor suspicious DLL loading and side-loading behavior.
- Restrict unnecessary kernel-driver installation and loading.

- Maintain an inventory of approved drivers and validate their digital signatures and provenance.
- Investigate unexpected security-service termination and driver-loading events.

Vulnerable Driver Mitigation

- Assess Windows endpoints for the presence of the identified vulnerable drivers.
- Investigate unexpected installation or loading of `ardrv.sys`, `ZYArKit.sys`, and `Alinubx.sys`.
- Apply relevant vendor security updates and mitigations for CVE-2026-36425.
- Restrict driver installation to authorized administrative workflows.
- Use Microsoft vulnerable-driver blocklist and other supported driver-control mechanisms where applicable.
- Avoid deleting legitimate driver files solely based on filename matches; validate file hashes, signatures, paths and associated activity before remediation.

Network and C2 Monitoring

- Monitor and investigate DNS requests for `fluxorv[.]top`.
- Review outbound traffic involving ports 80, 443 and 9999 in the context of suspicious processes.
- Correlate network connections with process execution and endpoint telemetry.
- Apply blocking measures for confirmed malicious infrastructure through organizational DNS, proxy, firewall and EDR controls.
- Preserve relevant DNS, firewall, proxy and endpoint logs for incident investigation.

BGD e-GOV CIRT

Incident Response

If a potential infection is identified:

- Isolate the affected endpoint from the network while preserving evidence.
- Notify the organization's incident response and security operations teams.
- Preserve suspicious attachments, executable files, DLLs, driver files, memory captures and relevant logs.
- Investigate the presence of the identified mutexes and registry paths.
- Review driver installation and endpoint security process termination events.
- Hunt for additional compromised endpoints and related C2 communication.
- Reset credentials that may have been exposed and review privileged account activity.
- Rebuild or restore affected systems from trusted sources when compromise is confirmed and remediation requires it.

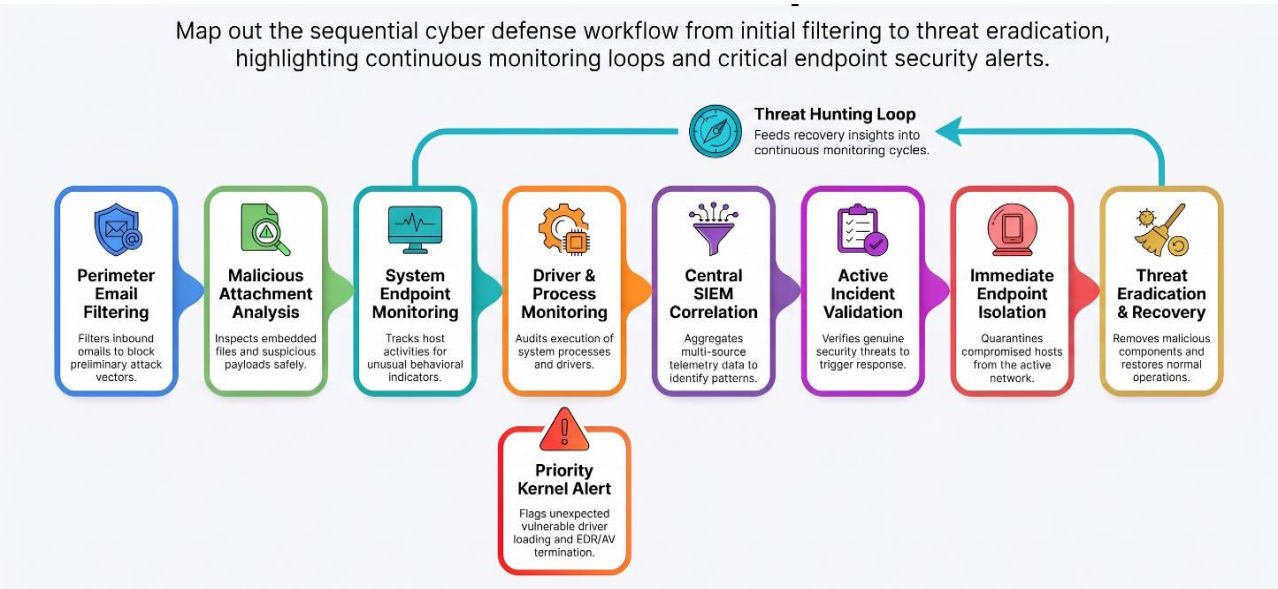


Figure: Recommended detection, containment and recovery workflow for organizations.

The FaCai campaign demonstrates how targeted phishing can be combined with trusted executable abuse, DLL side-loading, vulnerable driver exploitation and RAT deployment.

Organisations should prioritise the following defensive actions:

1. Treat unexpected VHD, IMG and ZIP attachments as potentially risky.
2. Investigate legitimate signed executables that load DLLs from untrusted or writable locations.
3. Monitor for vulnerable driver deployment and unexpected kernel-driver activity.
4. Protect antivirus and EDR processes against unauthorised termination.
5. Hunt for the supplied network, registry and mutex indicators.
6. Review suspicious outbound connections and preserve endpoint telemetry.
7. Report suspected compromise to the relevant incident response authority.

The FaCai phishing campaign represents a significant threat because it combines targeted social engineering with multiple techniques designed to establish persistent access and undermine endpoint security controls.

The use of DLL side-loading and Valley RAT-style payload delivery, together with vulnerable kernel drivers capable of terminating protected security processes, demonstrates a multi-stage intrusion approach.

Organizations in Bangladesh should proactively review their email security controls, endpoint protection configurations, driver inventories and network telemetry. Early identification of malicious attachments, suspicious DLL loading, vulnerable driver deployment and associated C2 communication will be essential to reducing the risk of compromise.

References

- MITRE ATT&CK – Phishing: Spearphishing Attachment (T1566.001).
- MITRE ATT&CK – Hijack Execution Flow: DLL Side-Loading (T1574.002).
- MITRE ATT&CK – Exploitation for Privilege Escalation (T1068).
- MITRE ATT&CK – Process Injection (T1055).
- MITRE ATT&CK – Ingress Tool Transfer (T1105).
- MITRE ATT&CK – Command and Control (TA0011)
- Group-IB Threat Intelligence – FaCai APT campaign analysis and technical findings

BGD e-GOV CIRT