JODOR Technologies

TLP:CLEAR

JODR MANAGED DECEPTION · TECHNICAL REPORT 2026

Machine-Speed Attack TTPs

Threat Alerting Report for SOC, threat intelligence and defence teams.
TLP:CLEAR.

ALERT ID JTI-2026-TA-01 · VERSION 1.0



OVERVIEW

Summary and actions today

What JODOR sensors observed, and five actions defenders can take today.

OBSERVED

2,207 hostile addresses from 84 countries hit JODOR sensors and deception systems in Saudi Arabia.

84% of known-exploit attackers (146 of 173) struck within 10 seconds of arriving.

50% of attackers (1,102 of 2,207) were on no public blocklist.

ACTIONS TODAY

1. Block the listed exploit paths at the edge.
2. Alert on deception and secret-file requests.
3. Patch CVE-2021-41773/42013, CVE-2024-4577 (and CVE-2012-1823), CVE-2021-3129, CVE-2017-9841.
4. Rotate any key that was ever in a web folder.
5. Expire address blocks after 30 to 90 days.

JODOR assessment: machine-speed exploitation of old flaws will almost certainly continue; act on the first request.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · JODOR detection rules, web_exploitation_rules_2026Q3.yar (TLP:CLEAR)

OVERVIEW

Where this data comes from

Context and definitions used throughout this report.

Term	Definition	Count
Sensors	Four types (deception web paths, service sensors, edge and web application firewall sensors, network sensors) in front of one live JODOR-operated web platform in Saudi Arabia, not a bank	56 days
Request	One web request logged with address, time, path and browser string	450,908
Visitor address	A distinct IPv4 or IPv6 source address	22,924
Attacker	An address JODOR confirmed hostile, or one that sent a known-exploit or secret-file request	2,207
Known-exploit attacker	Sent a request matching a published exploit pattern	173
Secret hunter	Asked for secret or configuration files (.env, .git/config, cloud keys, SSH keys)	261
On a blocklist	Matched at least one of 34 public blocklists	1,105
Country	First country recorded for the address (hosting location, not attribution)	84

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

OVERVIEW

How the observation ran

Sensors captured traffic for 56 days, and the AI agents were measured over 15 of those days.

TIMELINE (DURATIONS ONLY)

Sensor capture · 56 days

AI agents measured · 15 days

4

Sensor types deployed, built to look vulnerable, in front of one live JODOR-operated web platform in Saudi Arabia.

JODOR assessment: the agents acted alone, inside safety checks, for all 15 days. Every alert and block is counted once.

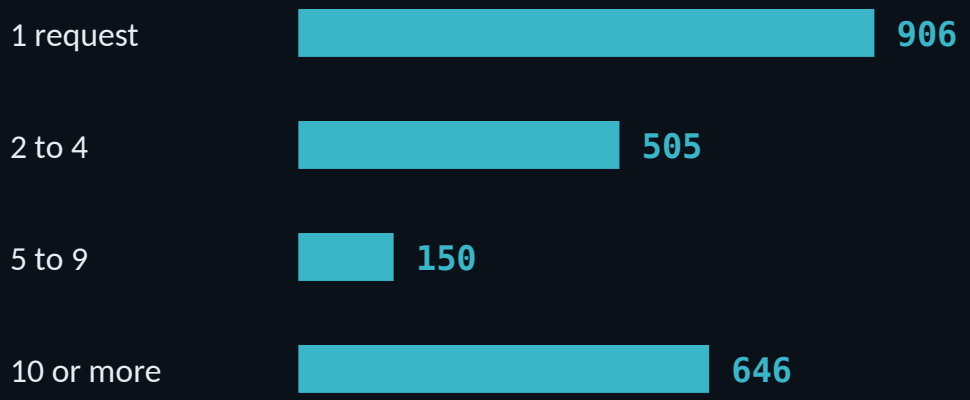
Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · JODOR AI analysis and rules data (JODOR analysis) · JODOR response data (JODOR analysis)

TECHNICAL DETAILS

Machine-speed tradecraft

Volume and timing per attacker, from web-log timestamps.

REQUESTS PER ATTACKER (n = 2,207)



Measure	Value
Five or more requests in one second	416 attackers
Peak requests in one second, one address	286
Ten or more paths within one minute	169 attackers
Known exploit within 1 second of arrival	64% (110 of 173)
Known exploit within 10 seconds	84% (146 of 173)
Median time to first secret-file request	0.75 s (n = 261)

JODOR assessment: timings are measured from each attacker's first logged request; logs alone cannot prove AI was used.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

TECHNICAL DETAILS

Attack families and CVEs

Exploit families seen, with request pattern, weakness and ATT&CK technique.

Family	Request pattern	Weakness	ATT&CK	Attackers
Secret and config files	`/.env*, /.git/config, /.aws/credentials, id_rsa, .htpasswd`	Credential exposure	T1552.001	261
Apache CGI traversal	`/cgi-bin/ + encoded ../ ending in bin/sh`	CVE-2021-41773, -42013	T1190, T1059.004	86
PHP-CGI argument injection	`allow_url_include + auto_prepend_file=php://input`	CVE-2024-4577, CVE-2012-1823	T1190	81
ThinkPHP code execution	`invokefunction + call_user_func_array`	ThinkPHP 5.x	T1190	59
Exposed Docker API	`/containers/json`	Misconfiguration	T1190, T1613	59
Spring Boot Actuator	`/actuator/env, heapdump, configprops`	Misconfiguration	T1552	58
Laravel Ignition	`/_ignition/execute-solution`	CVE-2021-3129	T1190	38
/etc/passwd traversal	`../../etc/passwd, /@fs/ pattern`	Generic traversal	T1190	17
PHPUnit eval-stdin	`vendor/phpunit/…/eval-stdin.php`	CVE-2017-9841	T1190	5

Rows overlap: one attacker can appear in several families. Known-exploit attackers in total: 173.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · CVE-2021-41773 · CVE-2021-42013 · CVE-2024-4577 · CVE-2012-1823 · VulnCheck, ThinkPHP invokefunction advisory · CVE-2021-3129 · CVE-2017-9841 · MITRE ATT&CK Enterprise matrix

TECHNICAL DETAILS

ATT&CK techniques seen

MITRE ATT&CK techniques mapped from behaviour on JODOR sensors.

Technique	ID	What JODOR sensors saw	Attackers
Exploit public-facing application	T1190	Exploit patterns against a public website or app	770
Unsecured credentials	T1552	Requests for secret, key and configuration files (wider set than the 261 secret hunters)	293
Command and scripting interpreter	T1059	Attempts to run shell or system commands on the server	145
Server software component: web shell	T1505.003	Attempts to plant or call a web shell	39
Valid accounts and brute force	T1078, T1110	Logins with stolen or guessed credentials	25
Container and resource discovery	T1613	Docker Engine interface probes	59
Active scanning	T1595	Automated path and weakness scanning at machine speed	Not counted

Counts use the 2,207-attacker base; one attacker can use several techniques.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · MITRE ATT&CK Enterprise matrix

TECHNICAL DETAILS

Attribution and blocklists

What the data says about who attacked, and what blocklists caught.

Question	Finding
Known state group?	None of the 2,207 matched a known state-linked group. No match is not proof of absence.
Blocklist coverage	50% (1,102 of 2,207) were on none of 34 public blocklists; matches came from commodity public lists.
Persistence	76% (1,687 of 2,207) were seen on one day only, then moved on.
Saudi-hosted sources	220 attackers were hosted in Saudi Arabia; 88% (194 of 220) were on no blocklist.
Disguise	Some visitors posed as search robots from networks the search engine does not use (see next slide, B01: 152 requests).

> **JODOR assessment:** these were very likely opportunistic, automated attackers; judge them by behaviour, not reputation.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published)

TECHNICAL DETAILS

Confirmed hostile infrastructure

Addresses confirmed hostile on JODOR deception systems, masked. Full list in the TLP:CLEAR pack.

Tier	Count	Selection rule	Hosting countries	Blocklists	Requests	Behaviour
A01–A16	16	On 2 or more public blocklists, plus a JODOR alert, plus exploit behaviour	US 6, DE 3, AD 3, GB 2, NL 1, SG 1	2–11	5–1,752	Code execution, file inclusion, SQL injection, deception hits, floods, scanning
B01	1	On no blocklist, plus a deception hit and an exploit attempt	CN	None	152	Posed as a search robot; swept configuration files and secrets
B02	1	On no blocklist, plus a deception hit and an exploit attempt	CH	None	23	Sweep of 15 or more .env variants

US United States · DE Germany · AD Andorra · GB United Kingdom · NL Netherlands · SG Singapore · CN China · CH Switzerland

JODOR assessment: address indicators age quickly; re-check them before blocking. Pack on request at info@jodr.sa.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · JODOR detection rules, web_exploitation_rules_2026Q3.yar (TLP:CLEAR)

DETECTION AND MITIGATION

JODOR detection rules

Eight of JODOR's 163 detection rules, published as YARA for web, proxy and firewall access logs.

```
rule PHP_CGI_Argument_Injection
{
  meta:
    author = "JODOR Technologies"
    mitre  = "T1190"
    tlp    = "CLEAR"
  strings:
    $a  = "allow_url_include" ascii nocase
    $b  = "auto_prepend_file" ascii nocase
    $c  = "php://input" ascii nocase
    $c2 = "php%3A//input" ascii nocase
  condition:
    $a and $b and ($c or $c2)
}
```

Rule	ATT&CK	Attackers
Web_Secrets_File_Sweep (needs per-client grouping)	T1552.001	261
Apache_CGI_Traversal_To_Shell	T1190, T1059.004	86
PHP_CGI_Argument_Injection	T1190	81
ThinkPHP_InvokeFunction_RCE	T1190	59
Docker_API_Exposure_Probe	T1190, T1613	59
Spring_Actuator_Sensitive_Sweep	T1552	58
Laravel_Ignition_RCE (execute-solution only)	T1190	38
Hostile_Web_Infrastructure_2026Q3 (18 masked addresses)	T1190, T1595	18

Run: yara rules.yar exported_access_log.txt. Group logs per client first for the secrets sweep rule.

Sources: JODOR detection rules, web_exploitation_rules_2026Q3.yar (TLP:CLEAR) · MITRE ATT&CK Enterprise matrix

DETECTION AND MITIGATION

Public rules worth running

Further detection for regional threats not seen in this data. Check each rule's date first.

Rule	Publisher, date, licence	Detects	Note
`apt_MuddyWater_MuddyRot_strings.yar`	Sekoia, Jun 2024, Detection Rule License 1.1	MuddyRot (BugSleep) strings in 100–300 KB files	Valid for the 2024 build
`apt_oilrig_odagent / sc5kv3_strings.yar`	Sekoia, Dec 2023	OilRig downloaders using cloud file storage and mail web services	Aging
`APT_MAL_IR_DruidFly_Wiper_Jun25`	signature-base, Jun 2025, Detection Rule License 1.1	Wiper attributed by the rule author	Attribution not independently confirmed
`MacOS_Trojan_RustBucket`, `MacOS_Backdoor_Applejeus`	Elastic, Elastic License 2.0	macOS tools used in finance-sector intrusions	
`Multi_Ransomware_RansomHub`, `Windows_Ransomware_Medusa`	Elastic, Elastic License 2.0	Ransomware configuration keys	
`win_software_atera_rmm_agent_install.yml (Sigma)`	SigmaHQ, Detection Rule License 1.1	Atera remote-access agent install (T1219.002)	Level high

Sources: Sekoia community rules · signature-base repository · Elastic protections-artifacts · SigmaHQ rules

DETECTION AND MITIGATION

Mitigations by technique

Each mitigation maps to a technique on the ATT&CK page; the last row covers automated response.

Technique	Mitigation
T1190	Patch internet-facing systems within 14 days; block the listed exploit paths at the edge.
T1059, T1505.003	Stop web processes from starting shells; watch web folders for new files.
T1552	Keep secrets out of web folders; use a vault; rotate keys; return 404 and alert on secret-file paths.
T1078, T1110	Require multi-factor authentication; rate-limit login attempts.
T1595	Detect by behaviour and deception; expire address blocks after 30 to 90 days; verify search robots by reverse lookup.
Response (all)	Let a rule agent block alone when the attack is proven and the block can be undone; have a person approve risky blocks that an AI model proposes.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · MITRE ATT&CK Enterprise matrix

DETECTION AND MITIGATION

Validate your controls

Test that your defences catch these attacks, in a staging environment.

- [ ] Replay the listed exploit paths against a staging edge, never production.
- [ ] Confirm an alert fires within 10 seconds of the first request.
- [ ] Check that secret-file paths return 404 and raise an alert.
- [ ] Confirm that address blocks expire on the date you set.
- [ ] Run JODOR rules over one day of your access logs and review every hit.

Sources: JODOR sensors and deception systems in Saudi Arabia (JODOR analysis; raw data not published) · JODOR detection rules, web_exploitation_rules_2026Q3.yar (TLP:CLEAR)

JODOR Technologies

TLP:CLEAR

JODR MANAGED DECEPTION · TECHNICAL REPORT 2026

Request the TLP:CLEAR rule and indicator pack

WEB	jodr.sa
EMAIL	info@jodr.sa
LINKEDIN	linkedin.com/company/jodr-technologies
OFFICE	Riyadh, Kingdom of Saudi Arabia

Email info@jodr.sa for the pack. Managed Deception subscribers receive this detail about their own attackers every month.

Scan to email info@jodr.sa