Encrypted traffic interception on Hetzner and Linode targeting the largest Russian XMPP (Jabber) messaging service

ValdikSS 20th October 2023 at 3:58pm

TL;DR: we have discovered XMPP (Jabber) instant messaging protocol encrypted TLS connection wiretapping (Man-in-the-Middle attack) of jabber.ru (aka xmpp.ru) service's servers on Hetzner and Linode hosting providers in Germany.
The attacker has issued several new TLS certificates using Let's Encrypt service which were used to hijack encrypted STARTTLS connections on port 5222 using transparent MiTM proxy. The attack was discovered due to expiration of one of the MiTM certificates, which haven't been reissued.
There are no indications of the server breach or spoofing attacks on the network segment, quite the contrary: the traffic redirection has been configured on the hosting provider network.
The wiretapping may have lasted for up to 6 months overall (90 days confirmed). We believe this is lawful interception Hetzner and Linode were forced to setup.

Last updated: 20 Oct 2023

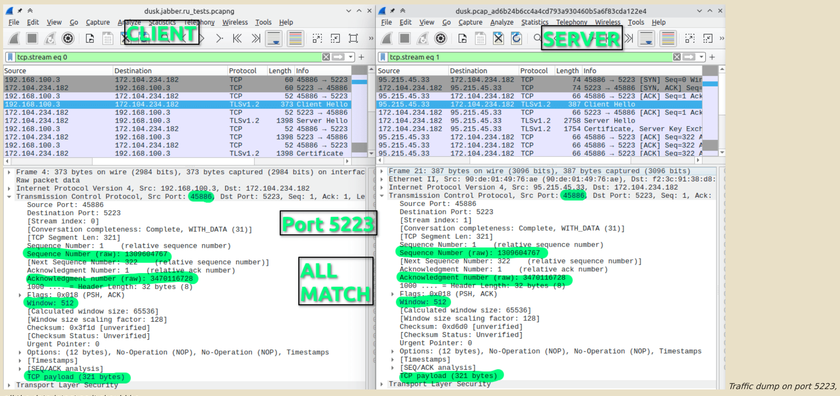
Introduction

`oxpa`, experienced UNIX administrator who is in charge for the oldest Russian XMPP service `jabber.ru` established in year 2000, was puzzled by "Certificate has expired" message upon connecting to the service on 16 October 2023. All the certificates seemed to be up-to-date on the server, but the connection to port 5222 (XMPP STARTTLS) was presenting an outdated certificate to the client.

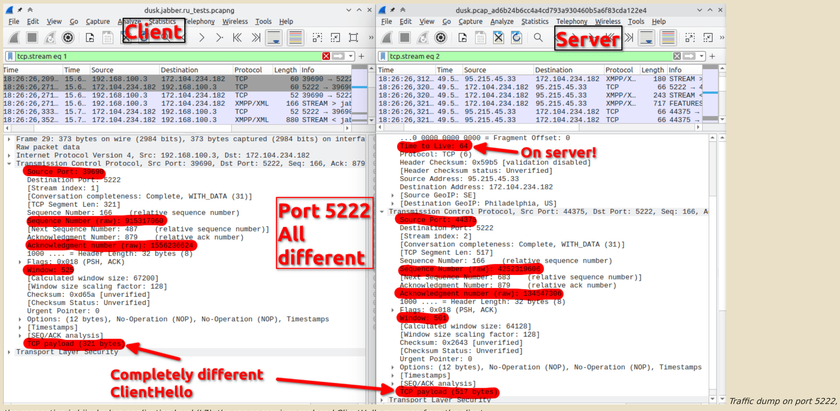
During all kinds of software, network and configuration checks with the help of other professionals and `ejabberd` software author, it was discovered that:

- The software serves proper, non-expired certificate in the network traffic
- The expired certificate is not present on the server
- It is based on other private key and was never issued by the server's `acme.sh` certificate issuing script
- Incoming TCP connections to port 5222 are altered: they have different source port, SEQ/ACK numbers, and appear to arrive without any intermediate routing hops (TTL=64).
- This behavior is not observed on other, non-5222 ports, such as 5223 XMPP TLS port

The affected machines are dedicated server on Hetzner and two virtual servers on Linode, all hosted in Germany.



Traffic dump on port 5223, all the data intact as it should be.



Traffic dump on port 5222, the connection is hijacked on application level (L7), the server receives replaced ClientHello message from the client.

Incident investigation

It was apparent that the connections on port 5222 are under Man-in-the-Middle attack which intercepts encrypted communications.

At first we had 2 hypothesis to check: whether the servers have been hacked and whether the traffic is altered due to some kind of local network (neighbor) spoofing.

For the server, we tested:

- All kind of logs
- Date of executable files and libraries modification
- Running processes, memory maps and "dangling" file descriptors of each of them
- Presence of userland `LD_PRELOAD` hijacking libraries with statically compiled `busybox`
- Presence of kernel-level hijacking modules by dumping the kernel memory with LiME and analyzing with volatility

But nothing stood out. We noticed the only uncommon record in the kernel log on Hetzner dedicated machine, it lost the physical network link for 19 seconds on 18 July 2023:

```
[Tue Jul 18 12:58:29 2023] igb 0000:04:00.0 enp4s0: igb: enp4s0 NIC Link is Down
[Tue Jul 18 12:58:48 2023] igb 0000:04:00.0 enp4s0: igb: enp4s0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX/TX
```

In addition, Linode machines are only used as a tunnel to Hetzner server as an alternative route, and are running only bare-bones basic services like SSH and NTP.
Yet we still see unaltered ServerHello packet from the Hetzner server in Hetzner↔Linode tunnel on Linode machine, which is alerted upon sending it to the client over Linode network interface. In other words, the encrypted connection interception of the same kind happens both on Hetzner dedicated and Linode VPS machines.

▸ Note about kernel memory dump

From the network perspective, we tested:

- Whether MAC address of the gateway have been altered with ARP spoofing
- Whether any single IP address in L2 segment replies multiple times for ARP request
- Whether rogue routing rules are present in the routing table (injected e.g. with ICMP redirect)
- Netfilter rules
- The presence of non-trivial-to-discover tunnels, such as IPsec (`ip xfrm`)

No sights of any hijacking by the network segment neighbors on either servers, nothing out of ordinary in the network configuration.
While it's still not uncommon to see insufficient spoofing protection on physical networks for dedicated servers, it's hard to believe that such sophisticated stealth spoofing is possible on a virtual infrastructure.

On the Linode machines there aren't any neighbors at all except the router. Affected Linode machines are unable to ARP-discover or ping any adjacent IP addresses in the same network segment which are perfectly functioning from the outside network.
"That's weird", I thought.

The unaffected (third-party) Linode VM can ping its neighbors. It is connected to the Cisco systems router:

```
# ip neigh
172.104.234.1 dev eth0 lladdr 00:00:0c:9f:f0:05 REACHABLE

OUI lookup:
00:00:0C Cisco Systems, Inc
```

However the affected VPS are connected to some unidentified MAC manufacturer:

```
# ip neigh
172.104.226.1 dev eth0 lladdr 90:de:01:49:76:ae REACHABLE

OUI lookup:
(no matches)
```

It became clear that the affected Linode VM have uncommon network setup compared to regular Linode instances, possibly have been isolated into separate VLAN.

Certificates

After checking `crt.sh certificate transparency database`, rogue certificates have been discovered which were not issued by any of jabber.ru servers.

There are two genuine certificates used in XMPP service: the one issued for `xmpp.ru, *.xmpp.ru` and the other one is for `jabber.ru, *.jabber.ru`.

The maliciously-issued certificates are slightly different from the regular ones for these domains: either the wildcard Subject Alternative Name is missing or a single certificate is issued for both `jabber.ru, xmpp.ru`. Moreover, MiTM configuration on xmpp.ru domain (which points to Linode servers) was slightly misconfigured: it serves only `xmpp.ru` certificate, yet the original server is configured to serve both `jabber.ru` and `xmpp.ru` certificates depending on requested XMPP domain.

List of rogue certificates:

Domain	Serial	Not Before	Not After	Used in MiTM
xmpp.ru	03:f3:68:ee:36:30:80:6a:07:81:17:81:04:0c:e3:d9:10:b1	Jul 18 12:49:03 2023 GMT	Oct 16 12:49:02 2023 GMT	+
xmpp.ru	04:9c:2d:af:cc:61:88:d6:67:9f:8b:97:99:ce:ad:c9:b7:e0	Oct 13 11:21:30 2023 GMT	Jan 11 11:21:29 2024 GMT	+
jabber.ru	03:43:75:1f:3d:80:20:7d:11:f5:61:98:5b:87:a7:37:81:c6	Apr 18 10:23:29 2023 GMT	Jul 17 10:23:28 2023 GMT	?
jabber.ru	04:4c:1c:8a:f4:37:a0:5a:dd:83:9c:54:74:89:bd:b9:97:90	Jul 18 12:38:51 2023 GMT	Oct 16 12:38:50 2023 GMT	+
jabber.ru, xmpp.ru	04:d1:d2:5d:09:95:48:9b:d6:14:cc:81:91:df:ac:7f:ec:c6	Apr 25 05:46:23 2023 GMT	Jul 24 05:46:22 2023 GMT	?
jabber.ru, xmpp.ru	04:b7:85:83:9a:fd:df:81:26:48:5b:34:28:08:53:d9:e6:79	Apr 25 06:04:19 2023 GMT	Jul 24 06:04:18 2023 GMT	+

18 July 2023 issuing time is about the same when Hetzner server has lost network link for several seconds.

We have a confirmation from the external network scanner that Linode servers started to serve `04:b7:85...` certificate on port 5222 since at least 21 July 2023. Unfortunately, this scanner doesn't process Hetzner ranges.

Network

We decided to run more network tests of Linode VPS from outside of the machine.

All adjacent Linode hosts are reachable by hop 13 from my laptop's internet connection.

```
# lft -d 22 172.104.226.23
Tracing .............*T
TTL LFT trace to 172-104-226-23.ip.linodeusercontent.com (172.104.226.23):22/tcp
 1  _gateway (192.168.100.1) 31.2ms
...
 9  a23-210-52-59.deploy.static.akamaitechnologies.com (23.210.52.59) 67.0ms
10  10.210.32.1 62.1ms
**  [neglected] no reply packets received from TTL 11
12  10.210.3.93 67.5ms
13  [target open] 172-104-226-23.ip.linodeusercontent.com (172.104.226.23):22 67.4ms
```

As well as hijacked port 5222 on `dawn.jabber.ru` Linode server:

```
# lft -d 5222 dawn.jabber.ru
Tracing .............**.T
TTL LFT trace to dawn.jabber.ru (172.104.226.29):5222/tcp
 1  _gateway (192.168.100.1) 29.3ms
...
 9  a23-210-52-57.deploy.static.akamaitechnologies.com (23.210.52.57) 64.9ms
10  10.210.32.2 64.7ms
**  [neglected] no reply packets received from TTL 11
12  10.210.1.235 60.7ms
13  [target open] dawn.jabber.ru (172.104.226.29):5222 60.2ms
```

However all other non-hijacked ports, such as SSH port 22, is reachable only via additional non-disclosed hop and now reachable only on hop 14:

```
# lft -d 22 dawn.jabber.ru
Tracing .............7*?**.?T
TTL LFT trace to dawn.jabber.ru (172.104.226.29):22/tcp
 1  _gateway (192.168.100.1) 28.8ms
...
 9  a23-210-52-57.deploy.static.akamaitechnologies.com (23.210.52.57) 65.4ms
```

```
10  10.210.32.2 66.2ms
**  [neglected] no reply packets received from TTL 11
12  10.210.1.235 61.7ms
**  [neglected] no reply packets received from TTL 13
14  [target open] dawn.jabber.ru (172.104.226.29):22 61.1ms
```

This means that the IP address of Linode VM have been placed behind additional machine which handles TCP port 5222 by itself and routes other ports to the real destination.

From inside the VPS it's not possible to establish new connections using source port 5222. The router does not reply for the packets originating from this source port, as well as doesn't send any ICMP error or Time-to-Live Exceeded for TTL=0 or TTL=1 outgoing packets.

```
# curl -v -4 --max-time 10 --local-port 5222 ifconfig.co

tcpdump:

23:37:46.116991 IP 172.104.226.29.xmpp-client > 172.64.170.5.http: Flags [S], seq 4385521, win 64240, options [mss 1360,sackOK,TS val 758380820 ecr 0,nop,wscale 7], length 0
23:37:47.135972 IP 172.104.226.29.xmpp-client > 172.64.170.5.http: Flags [S], seq 4385521, win 64240, options [mss 1360,sackOK,TS val 758381839 ecr 0,nop,wscale 7], length 0
23:37:49.189189 IP 172.104.226.29.xmpp-client > 172.64.170.5.http: Flags [S], seq 4385521, win 64240, options [mss 1360,sackOK,TS val 758383892 ecr 0,nop,wscale 7], length 0
```

STARTTLS termination

Using testssl.sh SSL/TLS testing script, it was discovered that the intercepting proxy accepts connections with anonymous ciphers on both Linode (xmpp.ru) and Hetzner (jabber.ru).
This is a rare (mis)configuration which could be used as one of the XMPP MiTM detection fingerprint. Regular SSL/TLS libraries are usually compiled without anonymous ciphers support, you won't be able to configure your service to use anonymous ciphers even if you explicitly allow it in configuration file most of the time, and it is confirmed to be not configured on the original server.

```
$ ./testssl.sh --starttls xmpp --xmpphost jabber.ru --standard --openssl-timeout 15 --connect-timeout 15 jabber.ru:5222

###########################################################
    testssl.sh       3.0.8 from https://testssl.sh/
    (abdd51d 2022-09-28 09:19:37)

    This program is free software. Distribution and
            modification under GPLv2 permitted.
    USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

     Please file bugs @ https://testssl.sh/bugs/

###########################################################

 Using "OpenSSL 1.0.2-bad (1.0.2k-dev)" [~179 ciphers]
 on val:./bin/openssl.Linux.x86_64
 (built: "Sep  1 14:03:44 2022", platform: "linux-x86_64")


 Start 2023-10-18 23:39:14        -->> 116.202.237.43:5222 (jabber.ru) <<--

 rDNS (116.202.237.43):  utro.jabber.ru.
 Service set:            STARTTLS via XMPP (XMPP domain=\'jabber.ru\')

 Testing cipher categories

 NULL ciphers (no encryption)                not offered (OK)
 Anonymous NULL Ciphers (no authentication)  offered (NOT ok)  <--<--
...
```

We have tested about 20 other popular XMPP services for the same MiTM method with the same `testssl.sh` command and discovered no anomalies (no support for Anonymous NULL Ciphers).

Summary and finale

- The attacker managed to issue multiple SSL/TLS certificates via Let's Encrypt for jabber.ru and xmpp.ru domains since 18 Apr 2023
- The Man-in-the-Middle attack for jabber.ru/xmpp.ru client XMPP traffic decryption confirmed to be in place since at least 21 July 2023 for up to 19 Oct 2023, possibly (not confirmed) since 18 Apr 2023, affected 100% of the connections to XMPP STARTTLS port 5222 (not 5223)
- The attacker failed to reissue TLS certificate and MiTM proxy started to serve expired certificate on port 5222 for jabber.ru domain (Hetzner)
- The MiTM attack stopped shortly after we begun our investigation and network tests on 18 Oct 2023, along with tickets to Hetzner and Linode support team, however passive wiretapping (additional routing hop) is still in place at least on a single Linode server
- Neither servers appear to be hacked
- Both Hetzner and Linode network appear to be reconfigured specifically for this kind of attack for the XMPP service IP addresses

All jabber.ru and xmpp.ru communications between these dates should be assumed compromised. Given the nature of the interception, the attacker have been able to execute any action as if it is executed from the authorized account, without knowing the account password. This means that the attacker could download account's roster, lifetime unencrypted server-side message history, send new messages or alter them in real time.

End-to-end encrypted communications, such as OMEMO, OTR or PGP, are protected from the interception only if both parties have validated the encryption keys. The users are asked to check their accounts for new unauthorized OMEMO and PGP keys in their PEP storage, and change passwords.

We tend to assume this is lawful interception Hetzner and Linode were forced to setup based on German police request.
Another possible, although much more unlikely scenario is an intrusion on the internal networks of both Hetzner and Linode targeting specifically jabber.ru — much harder to believe but not entirely impossible.

As of 20 Oct 2023, we're still waiting for the adequate reply from Hetzner and Linode to our inquiries.

Could you prevent or monitor this kind of attack?

There are several indications which could be used to discover the attack from day 1:

- All issued SSL/TLS certificates are subject to certificate transparency. It is worth configuring certificate transparency monitoring, such as Cert Spotter (source on github), which will notify you by email of new certificates issued for your domain names
- Limit validation methods and set exact account identifier which could issue new certificates with Certification Authority Authorization (CAA) Record Extensions for Account URI and Automatic Certificate Management Environment (ACME) Method Binding (RFC 8657) to prevent certificate issue for your domain using other certificate authorities, ACME accounts or validation methods
- Monitor SSL/TLS certificate changes on all your services using external service
- Monitor MAC address of default gateway for changes
- "Channel binding" is a feature in XMPP which can detect a MiTM even if the interceptor present a valid certificate. Both the client and the server must support SCRAM PLUS authentication mechanisms for this to work. Unfortunately this was not active on jabber.ru at the time of the attack.