7777 Botnet – Insights into a Multi-Target Botnet | Bitsight

By Written by Gi7w0rm

Archived: 2026-04-05 16:43:17 UTC

Over the last month there have been some updates about the mysterious 7777 botnet—which was first mentioned in this post in October 2023. Until now, it was known that the botnet was made up of TP-LINK routers and that it was being used to execute very low volume and controlled brute force attacks on Microsoft 365 services targeting corporate accounts. In our continuous efforts to have all sorts of malware families under our radar, the 7777 botnet is no exception. Our research, a collaborative effort between Bitsight TRACE and the security researcher Gi7w0rm, has uncovered additional information about this botnet, the devices it affects, and the victims it claims.

The name 7777 or Quad7 botnet originated from the simple fact that all routers had the port 7777/tcp exposed with the banner `xlogin`:

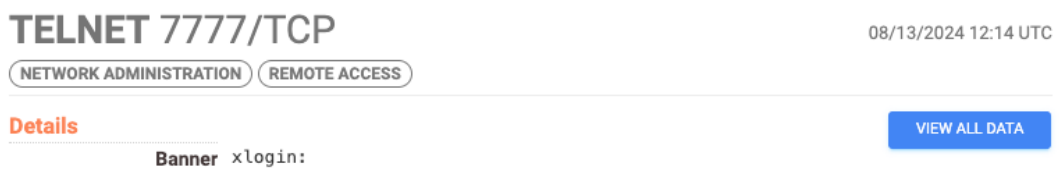

Figure 1: xlogin shell banner

In the latest update regarding this botnet, Team Cymru S2 revealed, a new cluster of routers that are also part of this botnet. This new cluster is made up of ASUS routers and all have port 63256/tcp exposed with the banner `alogin`:

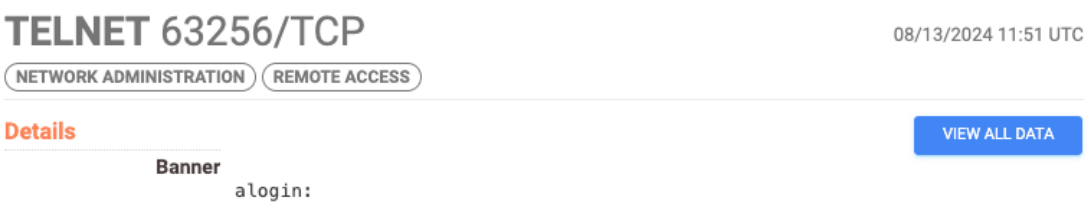

Figure 2: alogin shell banner

In this blog post, we will reveal two new but smaller clusters of compromised devices that feature bind shells exposing banners very similar to the already known `xlogin` and `alogin` banners that are also part of this botnet, and share some up-to-date infection telemetry.

Modus Operandi And New Clusters

After obtaining remote code execution on the devices, the threat actor installs a telnet binary that redirects connections to a bind shell that, after receiving the correct password, opens a new /bin/sh process. In addition to the bind shell that allows the threat actor to maintain direct access to devices, a SOCKS5 server is also installed on the devices so that they can be used as proxies in future brute force attacks.

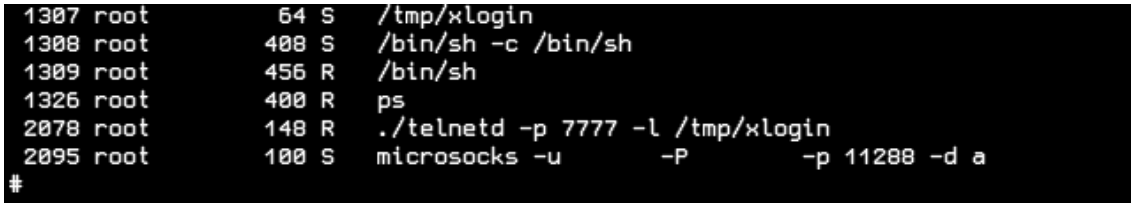

Figure 3: Running processes of a compromised TP-LINK router

All these artifacts installed on infected devices are placed within the /tmp directory which is volatile in memory. Whenever devices are turned off or restarted, their file system is reset and the contents of the /tmp directory are erased, which causes the threat actor to have to compromise the devices again.

It is worth mentioning that the entry vectors exploited by the threat actor are still unknown to us and trying to obtain this visibility is also not a trivial task as it implies two things:

1. have control over an IP that is on the threat actor's target lists
2. expose and monitor a vulnerable device, and hope for some luck

During our investigation we were able to identify two new but smaller clusters of compromised devices that are also part of this botnet. One of these clusters is made up of RUCKUS routers and these devices have port 63210/tcp exposed with the banner `rlogin`:

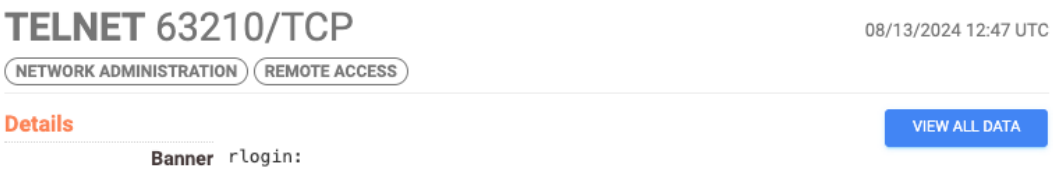

Figure 4: rlogin shell banner

The second cluster is even smaller and is made up of compromised Zyxel Firewall appliances. These devices have either port 3256/tcp or port 3556/tcp exposed with the banner `zylogin`:

Figure 5: zylogin shell banner

In the image below you can see what happens to the devices in the case of a successful exploitation attempt.

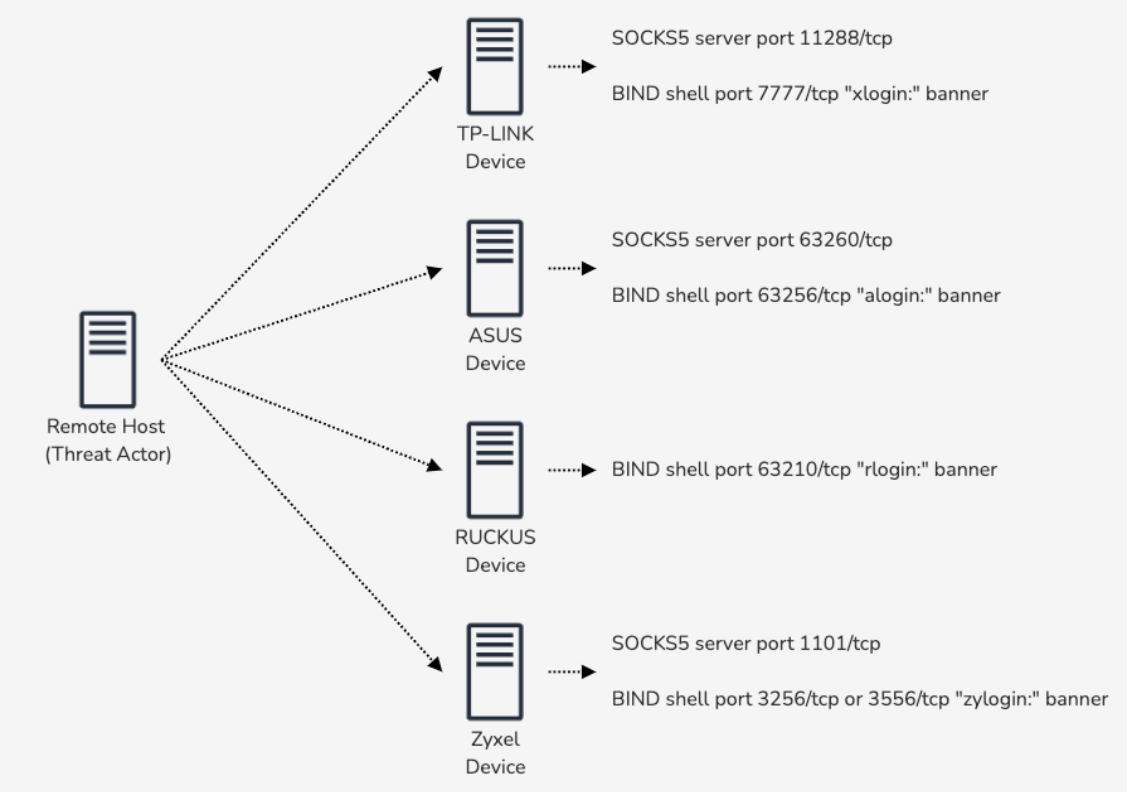

Figure 6: Exploitation result by device

We found an additional bind shell binary belonging to this threat actor's tooling that exposes the `axlogin` : banner.

```
1  int __fastcall sub_10254(int a1, int a2, int a3)
2  {
3    char v6[16]; // [sp+14h] [bp-78h] BYREF
4    char v7[104]; // [sp+24h] [bp-68h] BYREF
5
6    sub_10334("axlogin:");
7    sub_11688("%s", v7);
8    strcpy(v6, [redacted]);
9    if ( sub_118B0(v7, v6) )
10     sub_102F8("/tmp/login", a2, a3);
11   else
12     sub_12D68("/bin/sh");
13   return 0;
```

Figure 7: axlogin bind shell

We confirmed that this bind shell was used to backdoor Axentra devices, although no devices were found displaying this banner, likely because the company and its products have been discontinued for a long time now.

Based on available data, it is estimated that the botnet may have compromised more than **175.000 devices** since it began operating. During the last 30 days, through our internet scans, we were able to identify a total of around 16.000 infected devices with exposed bind shells. The fact that all infections are ephemeral, ie. require re-exploitation whenever a device is turned off or restarted, and that only about 9% of the devices remain infected to this day could be seen as an indicator that the threat actor has not been updating its targets for some time now. Still, we are looking at a decent sized and low profile botnet that has allowed the threat actor to conduct various brute force attacks to this day.

The top 5 countries with the highest number of compromised devices are in order:

- US (3103 devices)
- RU (2109 devices)
- BG (1390 devices)
- UA (1286 devices)
- PL (689 devices)

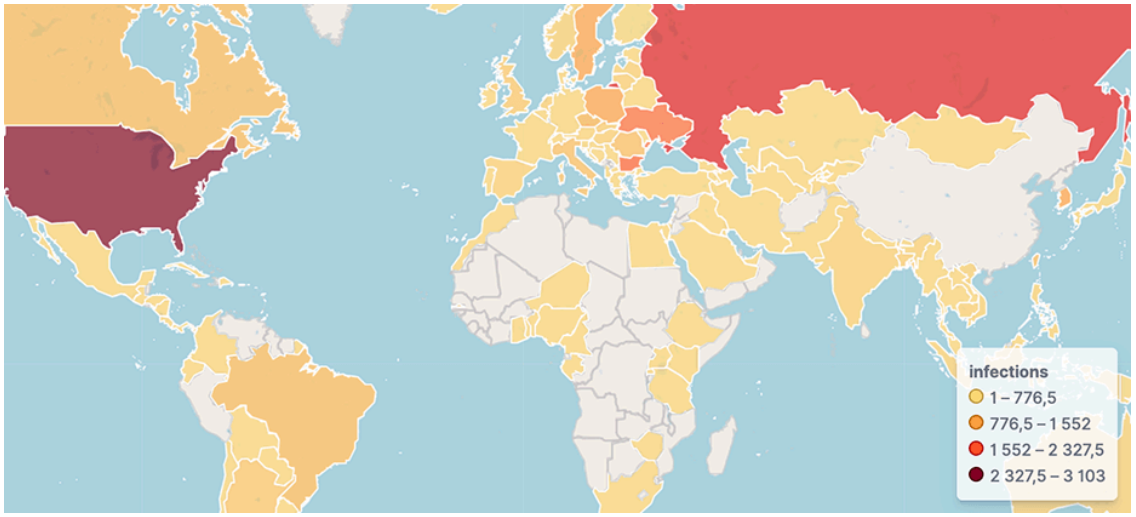

Figure 8: TP-LINK, ASUS and RUCKUS devices

As a botnet that is essentially targeting consumer devices such as routers, the expectation is that it would mostly affect residential users. Although the majority of cases align with our expectations, it is quite interesting to note that of the 840 organizations that we identified with at least one infected device, approximately 20% are not Internet Service Providers (ISPs). It is quite concerning to also see that there are infected devices belonging to Government institutions, many of them present in the USA.

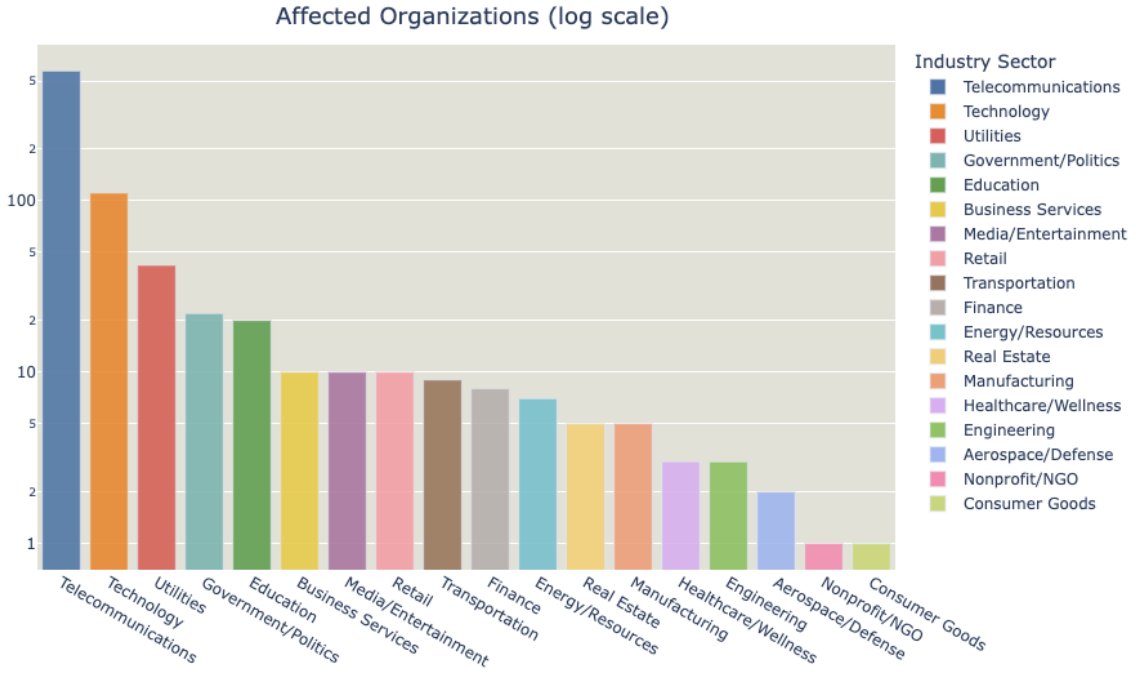

Figure 9: Affected Industry sectors

7777 cluster victims

The 7777 cluster of TP-LINK routers has around 8.303 infected devices and the top 5 affected countries remain the same, although the order changes.:

- BG (1340 devices)
- RU (1192 devices)
- UA (967 devices)
- US (829 devices)
- PL (410 devices)

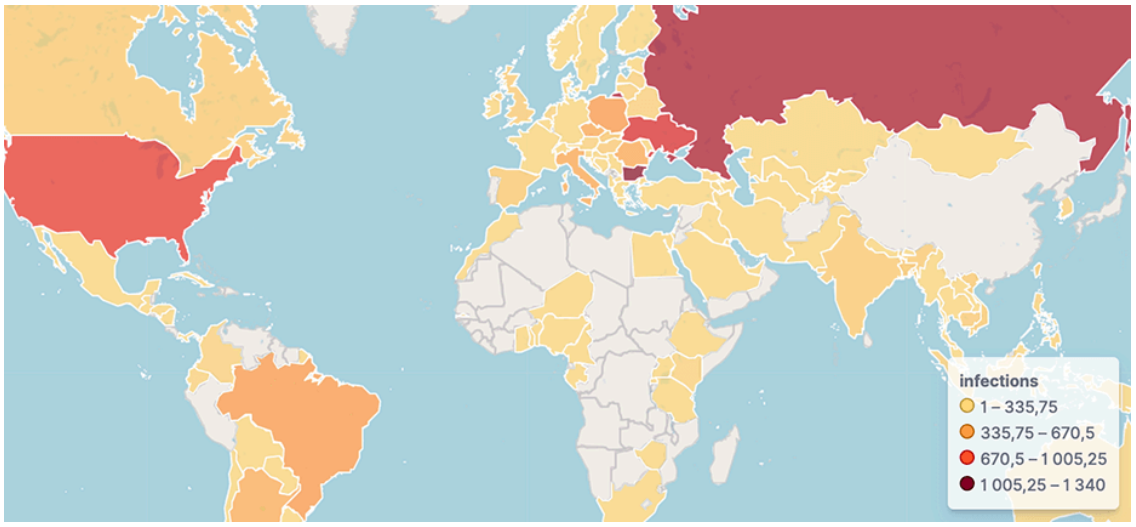

Figure 10: TP-LINK devices

63256 cluster victims

The 63256 cluster of ASUS routers has around 7.192 infected devices and here the top 5 affected countries already change a little:

- US (2210 devices)
- RU (917 devices)
- SE (625 devices)
- KR (471 devices)
- HK (406 devices)

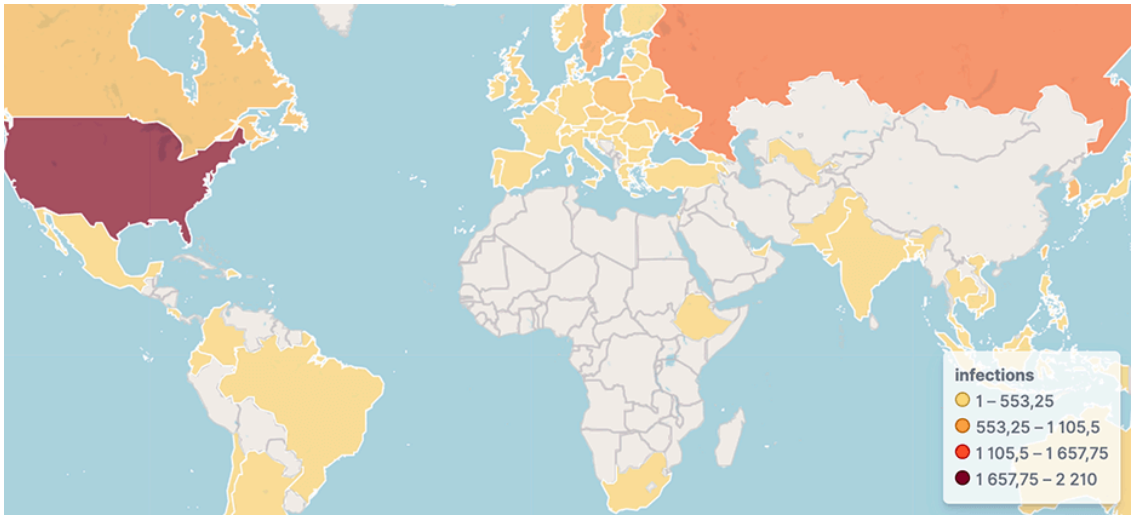

Figure 11: ASUS devices

63210 cluster victims

The 63210 cluster of RUCKUS routers has less than 200 infected devices and the top 3 affected countries are:

- KR (80 devices)
- US (56 devices)
- TW (5 devices)

Figure 12: RUCKUS devices

3256/3556 cluster victims

This cluster of compromised Zyxel devices is particularly interesting because only a total of 4 compromised hosts have been identified, all located in Hong Kong.

During our investigation of this botnet, we were able to identify a very significant number of device models that have been compromised. The diversity of affected models highlights the good capacity that this threat actor has to exploit vulnerabilities, which leads us to believe that this botnet could be part of an operation with good resources and capable of targeting devices of various brands and models.

The following models were found to be compromised:

ASUS	TP-LINK	Zyxel	RUCKUS
• 4G-AC53U • BLUE • BLUE_CAVE • DSL-AC68U • DSL-AX82U • GT-AC2900	• Archer-C7 • EC230-G1 • WDR-3500 • WDR-3600 • WDR-4300 • WR-1043ND	• USG20-VPN • USG60 • ZyWALL-11	• R500

ASUS	TP-LINK	Zyxel	RUCKUS
• GT-AC5300 • GT-AX11000 • GT-AX6000 • GT-AXE16000 • RT-AC1200 • RT-AC1200HP • RT-AC1300GPLUS • RT-AC1300UHP • RT-AC1750 • RT-AC1750_B1 • RT-AC1900 • RT-AC1900P • RT-AC3100 • RT-AC3200 • RT-AC51U • RT-AC51UPlus • RT-AC52U • RT-AC52U_B1 • RT-AC5300 • RT-AC54U • RT-AC55U • RT-AC55UHP • RT-AC56R • RT-AC56U • RT-AC58U • RT-AC66R • RT-AC66U • RT-AC66U_B1 • RT-AC66W • RT-AC67U • RT-AC68P • RT-AC68R • RT-AC68U • RT-AC68W • RT-AC750 • RT-AC85U • RT-AC86U • RT-AC87R • RT-AC87U • RT-AC88U • RT-ACRH13	• WR-740N • WR-840N • WR-841HP • WR-841N • WR-842N • WR-842ND • WR-843N • WR-845N • WR-940N • WR-945N • WR-949N		

ASUS	TP-LINK	Zyxel	RUCKUS
• RT-AX3000 • RT-AX56U • RT-AX58U • RT-AX68U • RT-AX82U • RT-AX86S • RT-AX86U • RT-AX88U • RT-AX89X • RT-AX92U • RT-N14U • RT-N14UHP • RT-N16 • RT-N18U • RT-N66R • RT-N66U • RT-N66W • TUF-AX3000 • TUF-AX4200 • TUF-AX5400 • WS880 • ZenWiFi			

There is some speculation regarding the purpose of this botnet and whether its activity is related to the interests of a particular state. At the moment, the only certainty that exists is that the botnet is being used to attack corporate accounts of interest through brute force attacks on Microsoft 365 services, always at a very low volume, in order to maintain a low profile and avoid detection.

There are some indicators publicly shared by the research community that suggest this botnet is likely operated by a threat actor originating from China. We were able to deeply investigate some of the infrastructure related to this botnet and, based on the evidence collected, we are very confident that this botnet is operated by a Chinese speaking threat actor.

We will continue to monitor the evolution of this botnet. If you are researching it and want to collaborate/exchange notes feel free to contact us at threat-research@bitsight.com.
