Ransomware Threat Landscape Quarterly

Trends and Insights in April-June 2024

11 July 2024

TLP: CLEAR
Disclosure is not limited

Clipeus Intelligence OU
Estonian Business Registration: 16862531
Harju maakond, Tallinn, Kesklinna linnaosa, Ahtri tn 12, 15551

Scope and Methodology

OSINT Monitoring

Data collection via monitoring of leak sites without actor engagement

Curated

We collect with automation but validate and enrich data with human intelligence

Time Scope

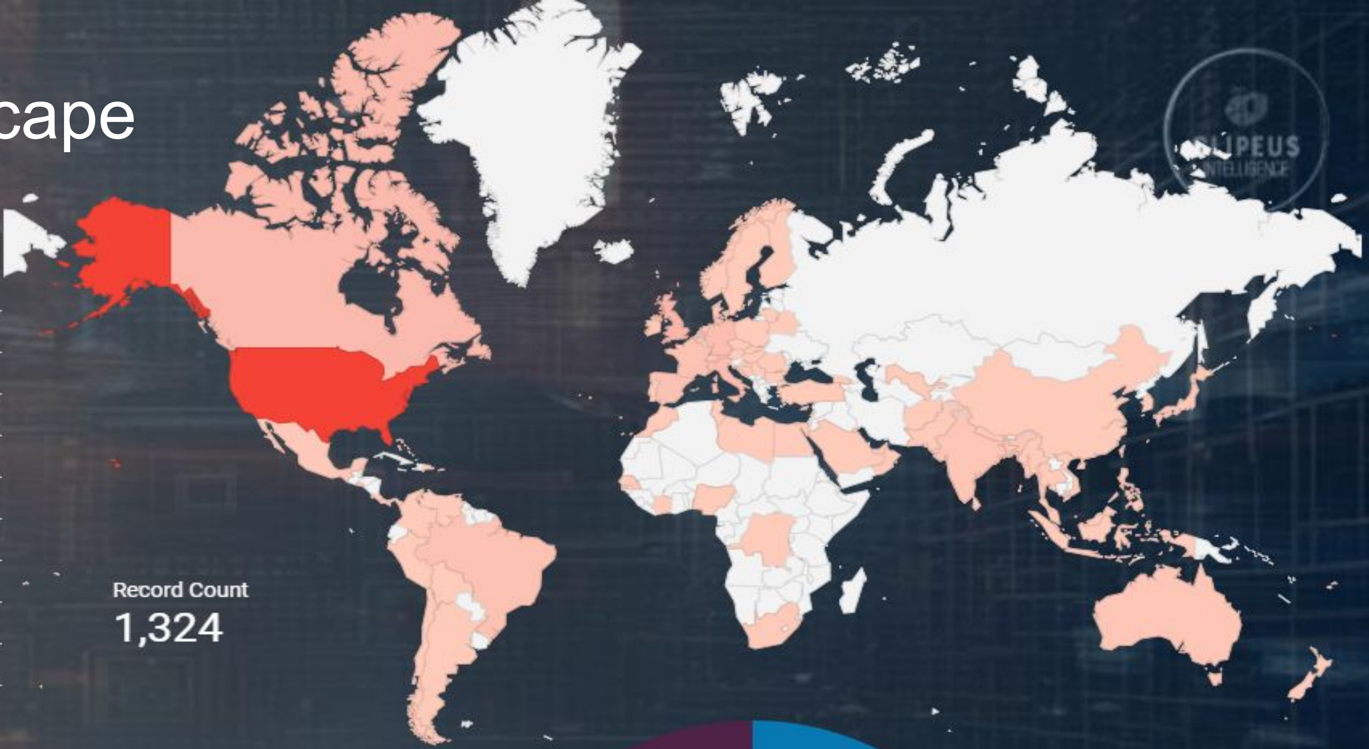
Our scope goes from April 1 to June 30, 2024, with insights of developments occurring in early July 2024

We developed a brand new web application for ransomware monitoring. Check it out here!

Threat Landscape

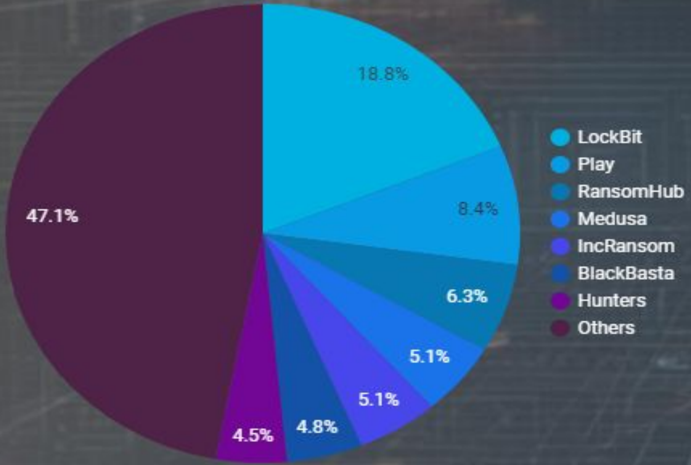
Overview

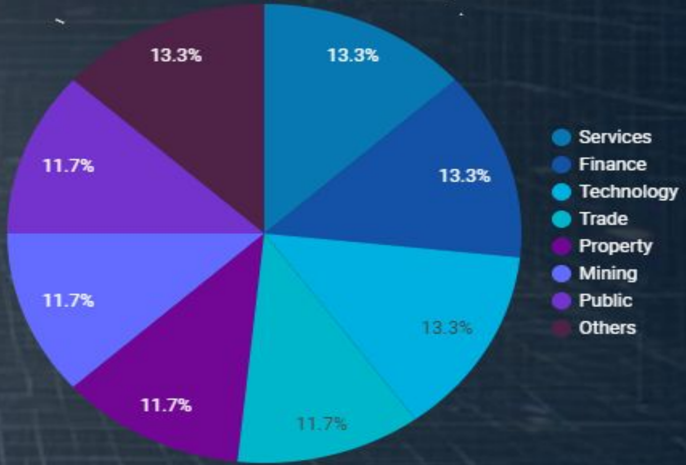
	Target Country	Record Count ▾
1.	United States of America	652
2.	United Kingdom	80
3.	Canada	68
4.	Germany	53
5.	Italy	51
6.	Brazil	39
7.	Spain	36
8.	France	33
9.	Australia	24
10.	India	23



Record Count

1,324





Threat Landscape

General Trends

Geopolitics continue to play a crucial role in the ransomware threat landscape, with military contractors being targets of breach claims. Several ransomware and extortion events appear to be politically motivated

SMEs are the most frequent targets of ransomware actors. Professional service providers, particularly in the legal, accounting, medical, and property management fields, are frequently found on data leak sites

Large corporations and governments are clearly high-value targets. It is critical for such entities to secure their **supply chains**, as numerous incidents originate via this vector

Ransomware Actors

Most Active Ransomware Operations By Volume Of Attacks

LOCKBIT
Claimed Victims: 249

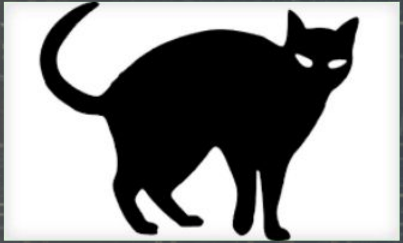
PLAY
Claimed Victims: 111

RANSOMHUB
Claimed Victims: 83

Despite the growing engagement of United States-led multinational law enforcement in disruptive initiatives, **LockBit** remains the primary actor in the ransomware threat landscape, even **growing its activity volume by 25.1 percent** from 1Q to 2Q 2024.

Evolution Of The Landscape

The Rise Of RansomHub



```
ransomhub:~#
```

RansomHub emerged in February 2024, during a timeframe approximately consistent with BlackCat's exit. Shortly afterwards, RansomHub offered for sale data stolen from a major US-based healthcare provider, suggesting the group may be a rebrand of BlackCat.

Furthermore, RansomHub ransomware presents considerable commonalities with Knight (formerly Cyclops) ransomware; RansomHub operators likely bought the Knight payload in February 2024 and customized it.

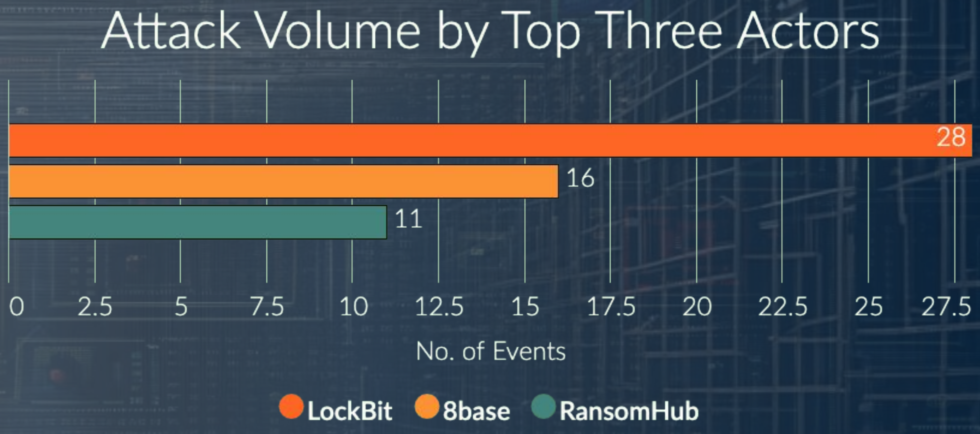
Regional View

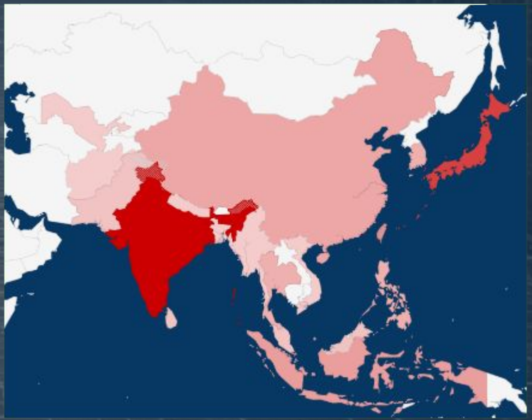
Asia

During the last quarter, India was the most targeted country for ransomware events, with a volume unusually high compared to the previous quarter when incidents were approximately aligned with China; notably, in 2Q2024, India and Japan surpassed China in observed events.

LockBit remains the primary threat in the region, while 8base doubled its attacks compared to 1Q2024. Consistent with a global trend, RansomHub emerged as a major player.

Notable events included the compromise of a telecommunications company in Thailand and a commercial bank in Indonesia.





Regional View

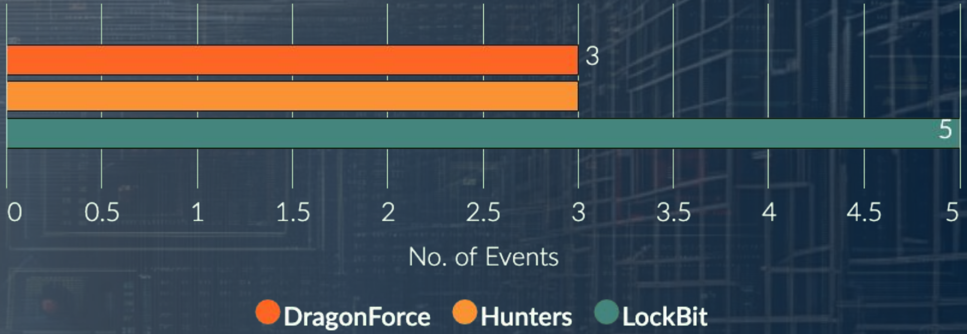
Oceania

During 2Q2024, ransomware events targeting Australia increased considerably (by 37 percent), while those against New Zealand dropped significantly. Fiji was the target of a single event.

LockBit is the main threat in the region, with Hunters and DragonForce following in attack volume.

Major events included Akira purportedly breaching the Australian branch of a high-profile Japanese technology conglomerate.

Attack Volume by Top Three Actors



Regional View

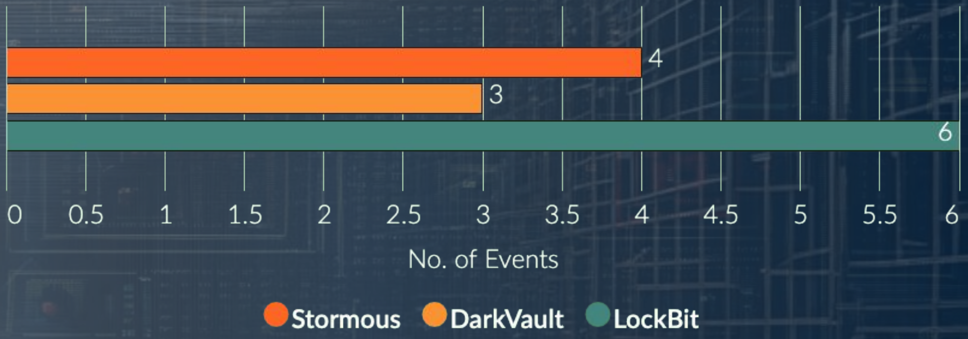
Middle East

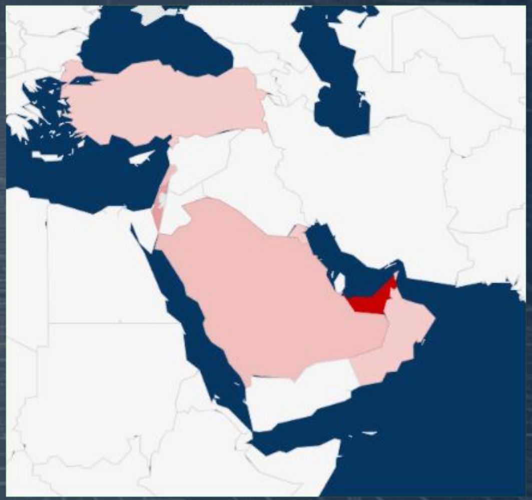
The United Arab Emirates has consistently been the primary target in the region. Saudi Arabia, Lebanon, and Oman were affected to a lesser extent.

Consistent with the global trend, LockBit is the primary threat actor in the region, followed by Stormous and DarkVault, which may have connections with the LockBit network.

Various events targeted Israel. The Malek Team, a politically motivated actor believed to be linked to Iran, remains the primary threat to Israel.

Attack Volume by Top Three Actors





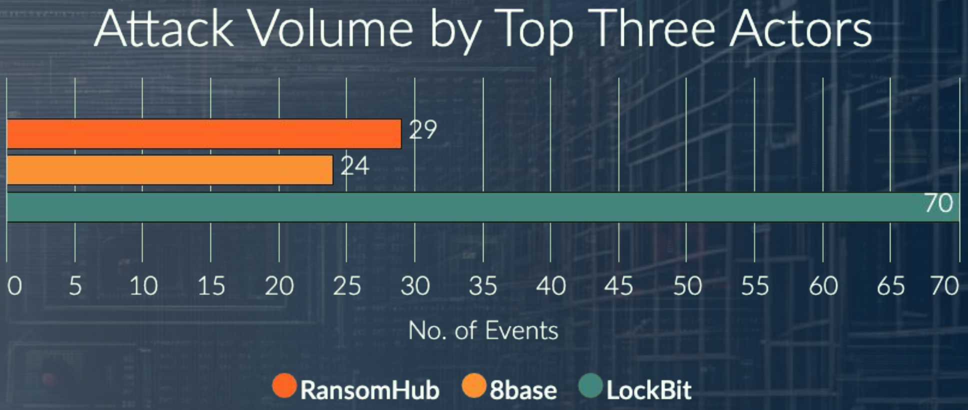
Regional View

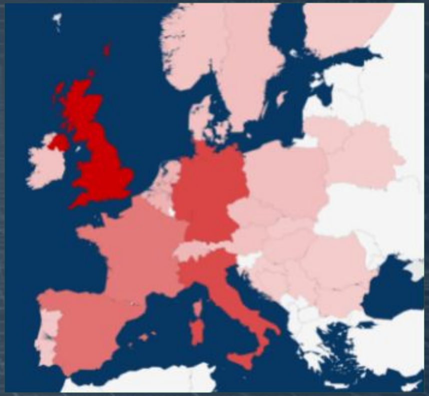
Europe

While the United Kingdom and Germany remain the most targeted countries, events against Italy doubled in comparison to last quarter, marking a significant escalation. There was a slight increase in attack volume in Spain, which in 2Q2024, neared the volume observed in France.

LockBit remains the main threat actor, followed by RansomHub, which continues to grow as a global threat. 8base remains a considerable regional threat.

Notable events include RansomHub claiming the compromise of a military technology provider and a major Italian cloud infrastructure provider, with potential impacts on various supply chains.





Regional View

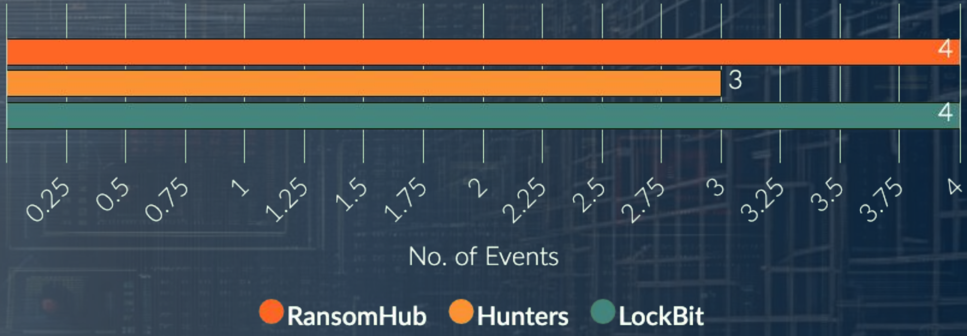
Africa

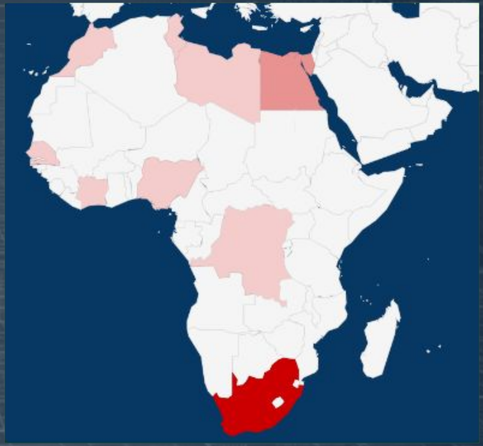
Quarterly data are consistent with a geographically broader targeting of African countries. While South Africa and Egypt remain the primary targets, attacks were claimed across the whole continent.

The growth of the ransomware threat in Africa appears to be a significant concern, particularly for entities engaged in the energy and mining sectors. Notable events observed in 2Q2024 include RansomHub claiming the breach of a Libya-based oil and gas conglomerate.

Alongside RansomHub, LockBit and Hunters are primary threats in the region.

Attack Volume by Top Three Actors





Regional View

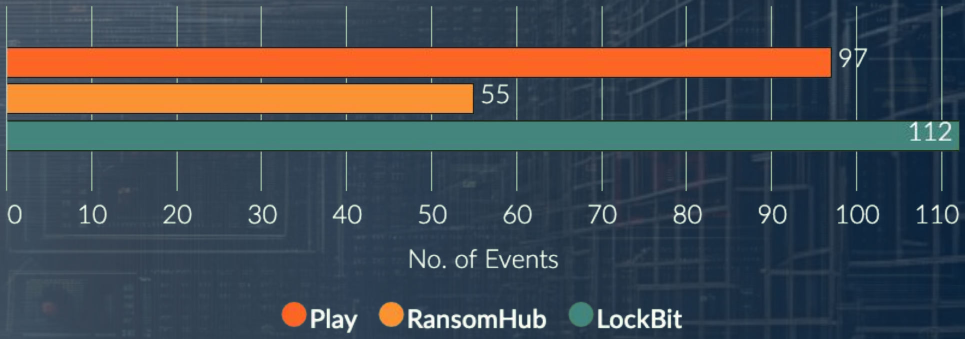
North-Central America and the Caribbeans

The volume of events targeting the United States increased by over 53 percent on a quarterly basis. Meanwhile, the volume of attacks against Mexico and Canada dropped slightly in the same timeframe.

The volume of LockBit attacks escalated by 24 percent, confirming the actor as the primary threat in the region. Play, with a volume of attacks nearing that of LockBit, emerges as the second most active actor, followed by RansomHub.

Critical sectors such as healthcare, local administration, military contractors, education, and SMEs remain consistently under threat.

Attack Volume by Top Three Actors



Regional View

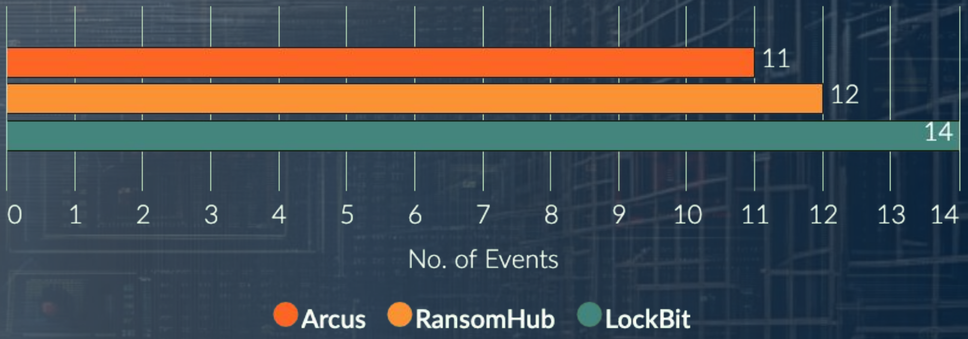
South America

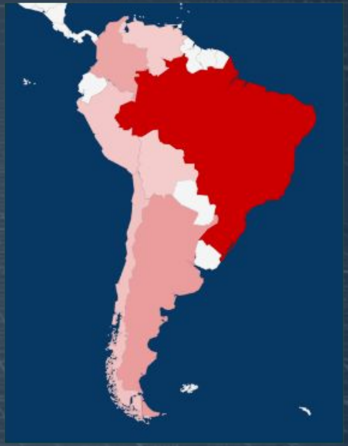
Brazil remains the primary target in the region, followed by Argentina and Colombia.

Consistent with the global trend, LockBit and RansomHub are the most active operations. 2Q2024 witnessed the emergence of new operations that displayed an unusual direction of interest towards the region, particularly Brazil. These include Arcus and Quilong. The latter exclusively targeted Brazilian healthcare service providers, particularly plastic surgery businesses.

Notable events include RansomHub claiming the compromise of a critical infrastructure operator in Brazil.

Attack Volume by Top Three Actors





The Defense Side

Attack Surface Management

Internet-facing appliances and corporate VPNs are frequent entry points for ransomware actors; BianLian targeted specifically **CVE-2024-3400**, impacting PAN-OS. In early July 2024, exploitation of **CVE-2024-6387** in OpenSSH was attributed to BlackSuit

BlackBasta has been linked to exploitation in the wild of **CVE-2024-26169**, a privilege escalation vulnerability affecting Windows Error Reporting Service

CVE-2023-22518, a critical vulnerability impacting Confluence Data Center and Server, has been exploited to deploy the Cerber ransomware

Initial Access Brokers

Recent Trends In The Ransomware Landscape

RustDoor, a Rust-based backdoor, has been reportedly linked to instances of LockBit ransomware infection

DanaBot and **PikaBot** loader have emerged as important initial access brokers (IABs), while **Qbot** remains present in the threat landscape

Raccoon stealer has been growingly observed as a major IAB across numerous ransomware events

Discover RansOmnia

Clipeus Intelligence Ransomware Intelligence Web Application

A tool developed by intelligence analysts for intelligence analysts. We aim to facilitate collection and analysis of ransomware intelligence

We enable executives and CISOs to visualize strategic intelligence and convey it effectively to C-level decision-makers

Our objective is to support CTI, threat hunting and SOC teams with actionable tactical and operational intelligence

Check it out here: Clipeus Intelligence | RansOmnia

This document is intellectual property of Clipeus Intelligence OÜ (thereafter only “Clipeus Intelligence” or "Clipeus"), an Estonia-registered limited liability company.

The document has been prepared by Clipeus Intelligence based on collection and analysis of open source intelligence and publicly available information. The document has been prepared respecting the criteria of legality and privacy policies presented on the company's website. Unless agreed with the client, no active collection technique has been employed. No engagement with any threat actor was conducted.

Clipeus Intelligence is committed to the betterment of communities and of the security ecosystem. In this spirit, intelligence is always shared with jurisdictionally-competent law enforcement whenever the company encounters information of potential illicit or criminal relevance.

Ransomware victim names were not reported, even if they were already disclosed via press or other online sources.

For questions, reach out to info@clipeusintelligence.com, or visit our website.

Clipeus Intelligence OU (registration: 16862531)

Harju maakond, Tallinn, Kesklinna linnaosa, Ahtri tn 12, 15551