SOCRadar®

AUGUST COMMS

Threat Landscape Report

SINGAPORE

June 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As new cyber threats emerge and the threat landscape grows, companies worldwide suffer more from critical cyber attacks each day, and companies in Singapore have seen their fair share of attacks.

SOCRadar Threat Landscape Report offers organizations a comprehensive understanding of evolving cyber threats and probable risks relevant to their geographical operating locations to enable security leaders to make better decisions.

The intelligence provided in this report could help organizations plan their enterprise-wide security programs, make investment decisions, and define cybersecurity requirements.

SOCRadar characterizes the threat landscape based on most recently observed threat actor activities, malware campaigns, new critical vulnerabilities, exploits, data gathered from open threat sharing platforms, and leveraging the comprehensive data monitoring, collection, classification, and analysis capabilities.

SOCRadar CTIA Team performs deep/dark web threat research, HUMINT observations, OSINT research, and analyses. SOCRadar can bring you the threat landscape report with its unique perspective on cyber incidents.

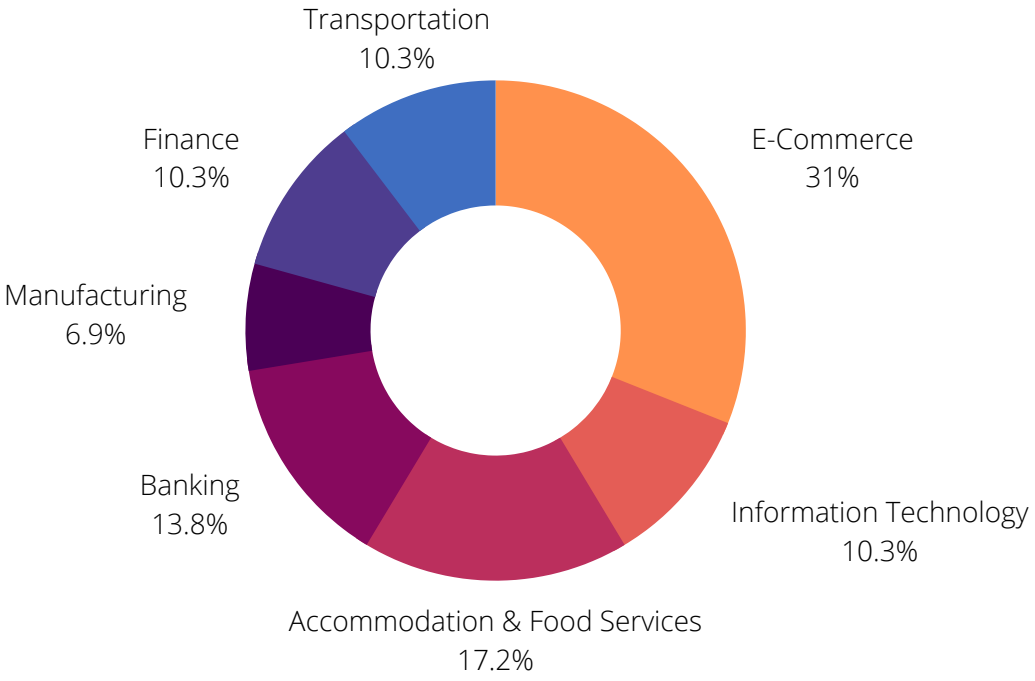
KEY FINDINDS

- **54 different threat actors targeting Singaporean enterprises shared posts on the dark web, and the most common post type was customer data sale.**
- **Top ransomware gangs targeting Singapore are Conti, LockBit 2.0, and AlphVM Blackcat.**
- **14 different APT groups have targeted Singaporean enterprises, and the Chinese government supports the top three most active APT groups in Singapore.**
- **SOCRadar has detected 7,644 phishing attacks targeting Singapore since the last year.**
- **Dark web marketplaces are crowded with compromised credentials of employees of Singaporean companies.**

Dark Web Threats

SOCRadar CTIA team has monitored the dark web to find trends and essential links between Singapore enterprises and threat actors lurking in the shadows. Throughout the last year, Singapore enterprises were bombarded with cyber attacks. Various threat actors have tried to sell and sometimes share the fruits of these successful cyberattacks on dark web hacker forums.

SOCRadar has detected 70 hacker forum posts belonging to 54 active threat actors throughout the last year. The most common threat actor post was customer data sale, but RDP access and network access sales were still present. The most commonly targeted industries were E-commerce and Accommodation & Food Services.



The most commonly targeted Industries in Singapore based on DarkMirror Intelligence data

54

Dark web threat actors / aliases

E-Commerce

The most targeted vertical

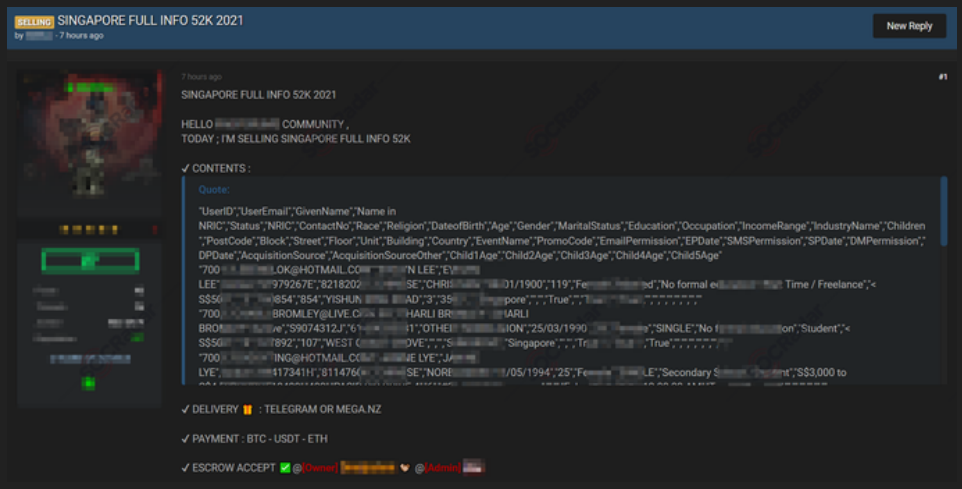
Customer Data Sale

Most common threat category

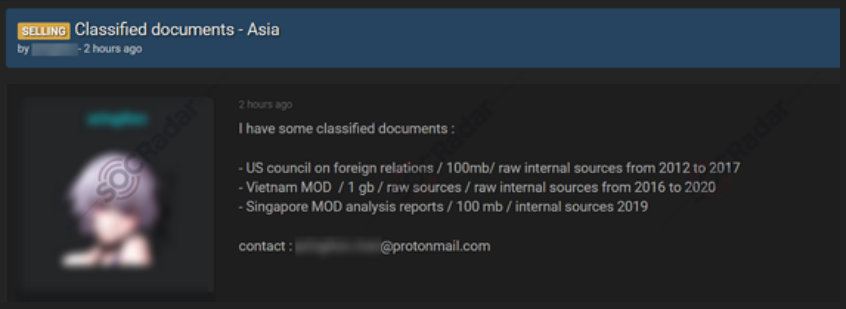
Major Dark Web Incidents

Database of Singapore Citizens is on Sale

On December 29th, 2021, a dark web hacker forum detected an alleged database sale of 52 thousand Singaporean citizens. According to the post owner, the database includes sensitive information such as legal name, date of birth, race, religion, age, gender, occupation, and education about Singapore citizens.



Database of Singapore Ministry of Defense are on Sale



On December 11th, 2021, SOCRadar's DarkMirror detected an alleged database sale by Singapore's Ministry of Defense, the US Council, and the Vietnam Ministry of Defense database sale. The threat actor did not specify details other than the size of the database, which was 100Mb for Singapore, and the contents of the database, which were analysis reports of the Ministry of Defense in 2019.

Network Access Sale Detected for a Sea Transportation Company

On July 9th, 2021, a threat actor posted an unauthorized network access sale of a Singaporean enterprise with 125M$ revenue. The company was a ship management service provider for international shipping.

Major Dark Web Incidents

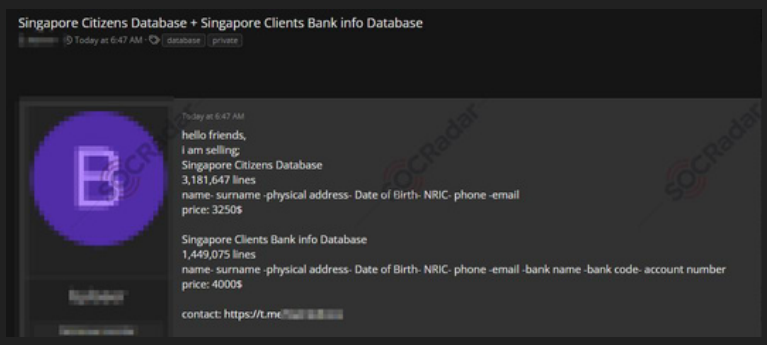
Employee Databases of Singapore Companies are Leaked

On January 13, 2022, Fifty-three thousand lines of data allegedly belonging to one of Singapore's leading companies, hacker forums followed by SOCRadar. Analysts stated that the data accessed via Snovio might belong to 2020.

Database of SingHealth is on Sale

On 28 March 2022, in a hacker forum monitored by SOCRadar, a new alleged database sale is detected for SingHealth. According to the information shared on the Telegram channels of SingHelath, one of the largest health organizations in the country, 1,507,913 lines of data were put up for sale. The threat actor asked for $2750 as the cryptocurrency for the data in question. SOCRadar analysts' analysis includes name, surname, date of birth, social security and citizenship numbers, contact information, and hospital information.

Bank Account Database of Singaporean Citizens is on Sale

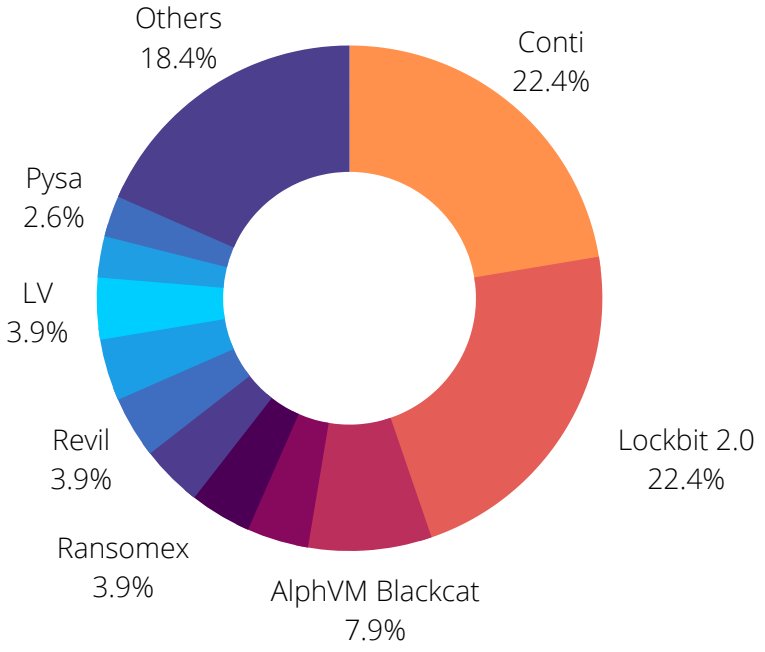


On 4 April, 2022, in a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Singaporean citizens. According to the information shared by SOCRadar researchers, it is stated that the size of the bank accounts of Singapore citizens on Telegram channels consists of 1,701,940 lines. The threat actor wanted $3500 in exchange for the data in question.

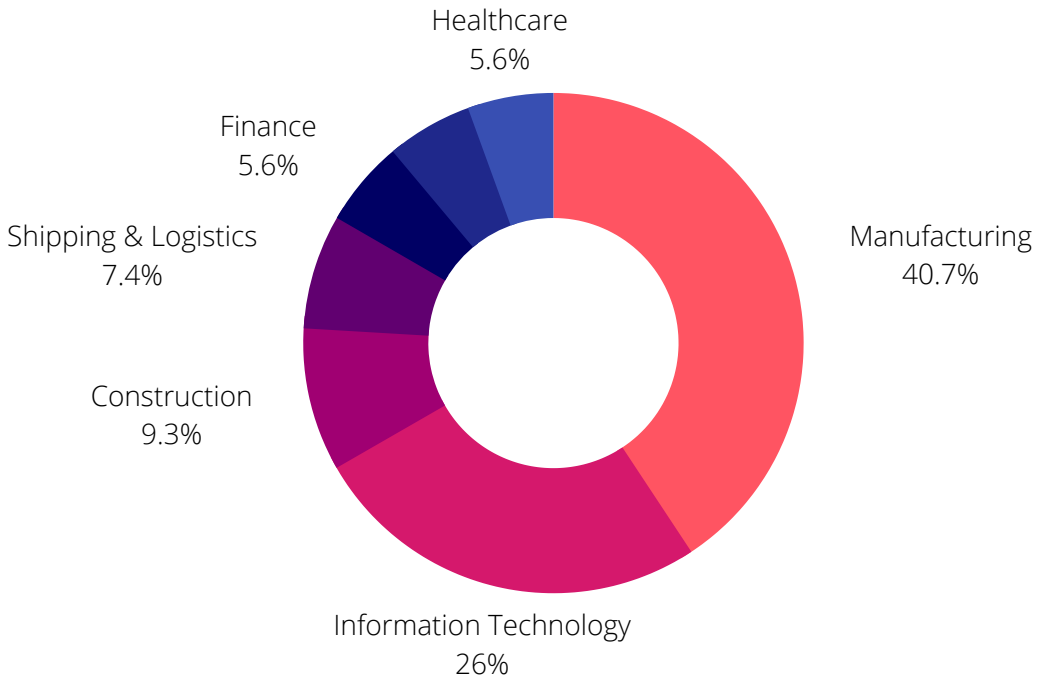
Ransomware Threats

Ransomware attacks are among the most critical cyber attacks an organization can experience. The results can be destructive for an organization and lead to massive data loss and leaks of the victim company's sensitive data. SOCRadar has detected 79 ransomware victim announcements belonging to diverse ransomware threat actors.

Conti, LockBit 2.0, and AlphVM Blackcat were the top three active ransomware gangs attacking Singaporean enterprises. The most commonly targeted industries by ransomware threat actors are Manufacturing, Information Technology, and Shipping & Logistics. According to SOCRadar's dataset, approximately 41% of ransomware victims' data are later leaked by the threat actor, showing that about 41% of Singaporean enterprises declined to pay the ransom.



Distribution of ransomware gang activities targeting Singapore organizations



Most targeted sectors in ransomware attacks

Top Ransomware Gangs Targeting Singapore

Conti

- Ransomware-as-a-service (RaaS) operator, believed to be originated in Russia.
- One of the most active ransomware gangs, Conti is actively targeting enterprises worldwide.
- After the gang's stand in the cyber-crisis between Russia and Ukraine, their internal chats and locker source code were leaked by a Ukrainian hacker who previously has gained access to Conti's internal systems.

LockBit 2.0

- Ransomware-as-a-service (RaaS) operator.
- Has one of the best-designed locker algorithms regarding encryption speed and overall functionality.
- The gang declared a newer version will come with upgraded functionalities and better capabilities, namely Lockbit 3.0.

AlphVM Blackcat

- First emerged on November 2021.
- Actively recruits ex Revil and ex BlackMatter members.
- The group's locker is written in Rust programming language, unlike other popular ransomware lockers.

State-Sponsored APT Activities

Advanced Persistent Threat (APT) groups are groups of threat actors who are generally directly sponsored by nations. Their goal may vary from carrying out malicious objectives of states to launching independent large-scale cyber attacks on critical infrastructures worldwide. Specific APT groups, mainly from China and Vietnam, have found numerous cyberattacks on Singapore's state-affiliated enterprises and non-state companies throughout the last year.

SOCRadar CTIA team has monitored and followed cyber trends regarding the activities in Singapore of various APT groups. SOCRadar has found that 14 different APT groups have been targeting Singaporean enterprises. The three of the top four most active APT groups in Singapore were believed to be supported by the Chinese government, and the fourth group is believed to be of Vietnamese origin.

Significant APT Groups Targeting Singapore

APT41 **APT30** **APT32** **APT1**

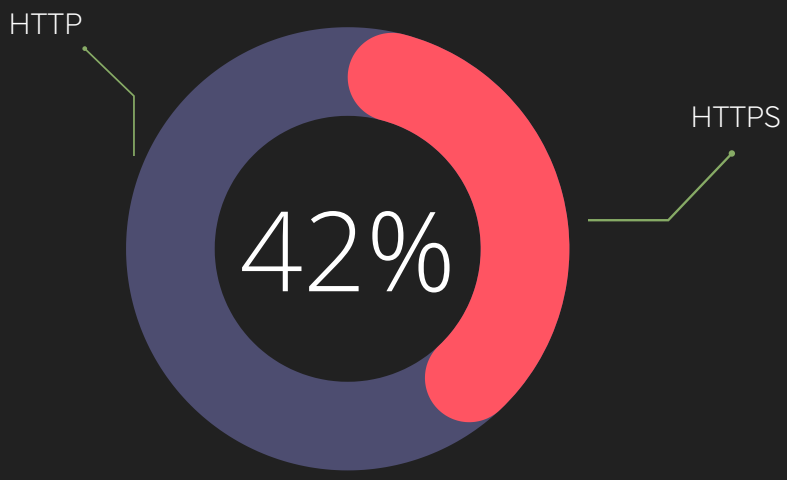
SOCRadar collects Advanced Persistent Threat (APT) IOC Feeds from several public and private sources and sensors. These feeds are free and refreshed daily.

DOWNLOAD

Phishing Threats

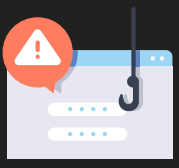
Phishing is a great way to gain initial access to an organization's infrastructure by tricking people into entering sensitive credentials into fake websites.

Phishing attacks are generally combined with social engineering attacks to obtain sensitive credentials. Throughout the last year, Singapore has experienced many phishing attacks. Most commonly imitated sectors were Shipping & Logistics, Information Technology, and E-Commerce sectors.



Attackers are increasingly using HTTPS to lure their victims into clicking malicious links

SOCRadar has collected and detected 7,644 phishing attacks targeting Singaporean organizations. Phishing attacks in Singapore continue to be a significant threat to Singaporean enterprises, resulting in potential cyber-attacks and breaches.



7644

Total phishing attacks detected throughout 2021

Shipping & Logistics
Information Technology
E-Commerce

Top targeted sectors in Singapore

Search On Phishing Radar

Enter your domain

Critical Asset Exposures & Vulnerabilities

In 2021, the number of vulnerabilities with a CVSS score higher than 8 was 929. Threat actors commonly exploit these vulnerabilities to launch critical cyber attacks on vulnerable enterprises. SOCRadar CTIA team has found that some Singaporean companies are still vulnerable to patched and deprecated critical vulnerabilities.

It is recommended that the following vulnerabilities are checked and patched if the vulnerability exists.

# of Vulnerable Hosts | CVE ID | CVSSv3

Critical Vulnerabilities commonly exploited in the last year affecting Singaporean Enterprises:

10	Microsoft Exchange Server Unauthenticated Remote Code Execution Vulnerability	CVE-2021-26855 #ProxyLogon	CVSS: 9.8
39	Microsoft Exchange Server Elevation of Privelege Vulnerability	CVE-2021-34523 #ProxyShell	CVSS: 9.8
	Apache Log4j2 Remote Code Execution Vulnerability	CVE-2021-44228 #Log4J	CVSS: 10.0
	Spring4Shell Remote Code Execution Vulnerability	CVE-2022-22965	CVSS: 9.8

Identity & Credentials Intelligence

Compromised credentials create high cyber risks, damaging companies' security posture. Threat actors may utilize stolen, compromised credentials to gain initial access to your enterprise, resulting in devastating cyber attacks. SOCRadar has detected more than 1 billion exposed credentials throughout the last year by monitoring the dark web and thoroughly analyzing breach datasets.

SOCRadar has crawled through dark web marketplaces to effectively measure the potential cyber risks emerging from compromised credentials in Singapore. The number of compromised credentials for sale is approximately 1,500.

Some of these credentials could even be login credentials of C-level associates or users with admin privileges. Compromised credentials could be leveraged to perform critical cyber-attacks.

CHECK FOR ACCOUNT BREACH Enter your domain/email

1,455
Compromised Credentials for sale | Singapore

6,382
Stealer Logs for sale | Singapore

2,247
Data Dumps for sale | Singapore

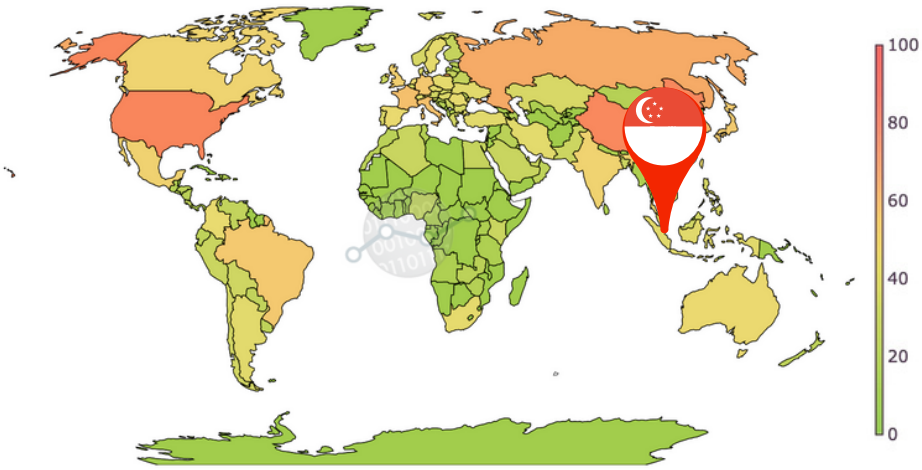
1,728
RDP Access for sale | Singapore

Source: Dark Web Marketplaces
Threat actors mainly use dark web marketplaces to buy/sell/share stolen credential intelligence, stealer log data, and sometimes initial access brokers.

DDoS | Risk-to-others

DDoS is among the most commonly executed cyber attacks, and Singaporean enterprises have experienced major DDoS attacks throughout the last year. As a result of a high volume of DDoS attacks, enterprises could experience significant financial losses due to critical service disruptions.

Singapore was ranked 30th in DDoS worldwide. Based on the global risk condition dataset provided by Cyber Green Initiative, Singapore can generate ~30TBit/sec DDoS traffic, colossal traffic that can disrupt the services of huge organizations.



Global heatmap view of total potential DDoS bandwidth by country

Data source: CyberGreen

CHECK FOR DoS RESILIENCE

Enter your domain/IP Block

30 TBit/Sec

Singapore | Total DDoS Potential

46,195
Open Recursive DNS

1,754
Open SNMP

50,084
Open NTP

38
Open CHARGEN

802
Open SSDP

ABOUT SOCRadar®

SOCRadar platform is an all-in-one solution that provides Extended Threat Intelligence, Digital Risk Protection, and External Attack Surface Management. Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with robust AI algorithms and a highly talented analyst team; together, they eliminate false positives.

FOLLOW US!

AUGUST COMMS

If you have a business in Singapore and want to benefit from the solutions offered by SOCRadar, you can contact our valued partner AugustComms in Singapore:
Address: August Communications Pte. Ltd., 8 Burn Road #15-13, 369977 Singapore
E-mail: sales@augcomms.com

DISCOVER SOCRADAR® FREE EDITION

With SOCRadar® Free Edition, you'll be able to:

- **Discover your unknown hacker-exposed assets**
- **Check if your IP addresses tagged as malicious**
- **Monitor your domain name on hacked websites and phishing databases**
- **Get notified when a critical zero-day vulnerability is disclosed**

TRY FOR FREE

CONTACT US info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709