SOCRadar®

'19 out of 53 Ransomware Victims Refused to Pay the Ransom'

THAILAND THREAT LANDSCAPE REPORT

OCTOBER 2022

'19 out of 53 Ransomware Victims Refused to Pay the Ransom'

With the effects of the pandemic disease of Covid-19, digital transformation has taken place throughout the world and in Thailand. The number of cyber-attacks has doubled since Covid-19. Therefore, it is evident that more Thai companies will devote themselves to cyber security in the future.

This report includes major critical points of various types of cyber incidents that the SOCRadar Platform relates to Thailand in September 2021 and September 2022. This country threat landscape report offers organizations in Thailand a comprehensive understanding of these evolving cyber threats and potential risks relevant to their geographical operating locations in Thailand 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 their cybersecurity requirements.

- SOCRadar DarkMirror has detected 14,534 dark web posts. 190 of these posts were related to organizations in Thailand.
- SOCRadar has detected "2,900 ransomware incidents" globally belonging to 52 distinct ransomware groups. 53 of these incidents belonged to organizations in Thailand.
- According to SOCRadars DarkMirror, "Government, Education, and Media & Entertainment" were Thailand's top three most targeted verticals in the last 12 months.
- "42,913 recursion-enabled devices" have been detected in Thailand within the specified time scope.
- With the intelligence that SOCRadar provides, it is observed that "590 different phishing attacks" have targeted Thai companies.
- "88,588 Thailand users" have been infected with Stealer (Redline, Raccoon, Vidar).
- "Almost 1 million credentials that access '.th' domains are leaked" from the users and are distributed on the dark web.
- "24 finished DDoS attacks" against Thailand that lasted more than one hour have been recorded.

ABOUT SOCRadar®

Who is SOCRadar?

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, our aim is to help security teams to detect blindspots before attackers.

To provide the "right blend" to the security teams, SOCRadar focuses on relative and actionable intelligence with minimized false positives. To generate the contextualized intelligence, SOCRadar's EASM service first maps out an organization's internet-facing digital assets with a hacker mindset and strengthens the organization's visibility on what to defend. The second integral part of the XTI is the DRP services with which SOCRadar provides monitoring capabilities across all environments. Besides monitoring, SOCRadar includes site takedown and automated remediation to its DRP services. The third leg of XTI is threat intelligence. Gathering intelligence from not only open sources and social media but also dark web forums along with other secret communication platforms attackers use, SOCRadar becomes the organization's eye on the dark side of the Internet.

Why Country Reports?

SOCRadar country threat landscape reports provide organizations with an understanding of evolving cyber threats relevant to their geographical operating locations to enable security leaders to make better decisions. The intelligence provided in this report can help plan enterprise-wide security programs, make investment decisions and define cybersecurity requirements.

SOCRadar characterizes the threat landscape based on recently observed threat actor activities, malware campaigns, recent critical vulnerabilities, exploits, data gathered from open threat sharing platforms, and leveraging the comprehensive data monitoring, collection, classification, and analysis capabilities of SOCRadar Platform. Country reports show that some regions remained a prime target for certain threat actors. Knowing the persistent actors with country reports can also enable organizations to take action against cyber threats more quickly.

ABOUT SOCRadar®

SOCRadar provides extended cyber threat intelligence (XTI) that combines,

- Cyber Threat Intelligence,
- Digital Risk Protection,
- External Attack Surface Management Services

SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Darknet and Deep Web Monitoring

SOCRadar's fusion of its unique dark web Recon technology with the human analyst eye achieves further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Credit Card Monitoring

Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

Protecting Customers' PII

Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.

360-Degree Visibility

Achieve digital resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

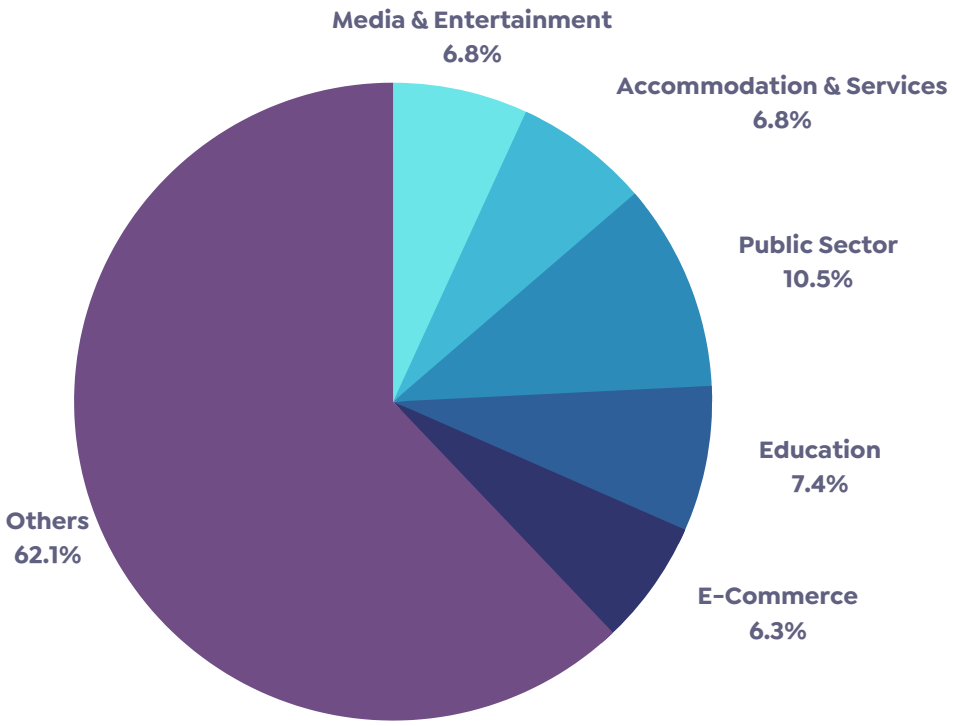
Dark Web Threats

SOCRadar monitored the dark web to collect actionable threat intelligence about the ever-changing cyber landscapes to inform organizations and enable them to take action against threat actors wanting to damage their enterprise.

Globally, within our time scope (September 15, 2021-September 15, 2022), SOCRadar DarkMirror has detected 14,534 dark web posts. 190 of these posts were related to Thai organizations. SOCRadars Dark Web Team has analyzed the bases to bring you the statistics below.

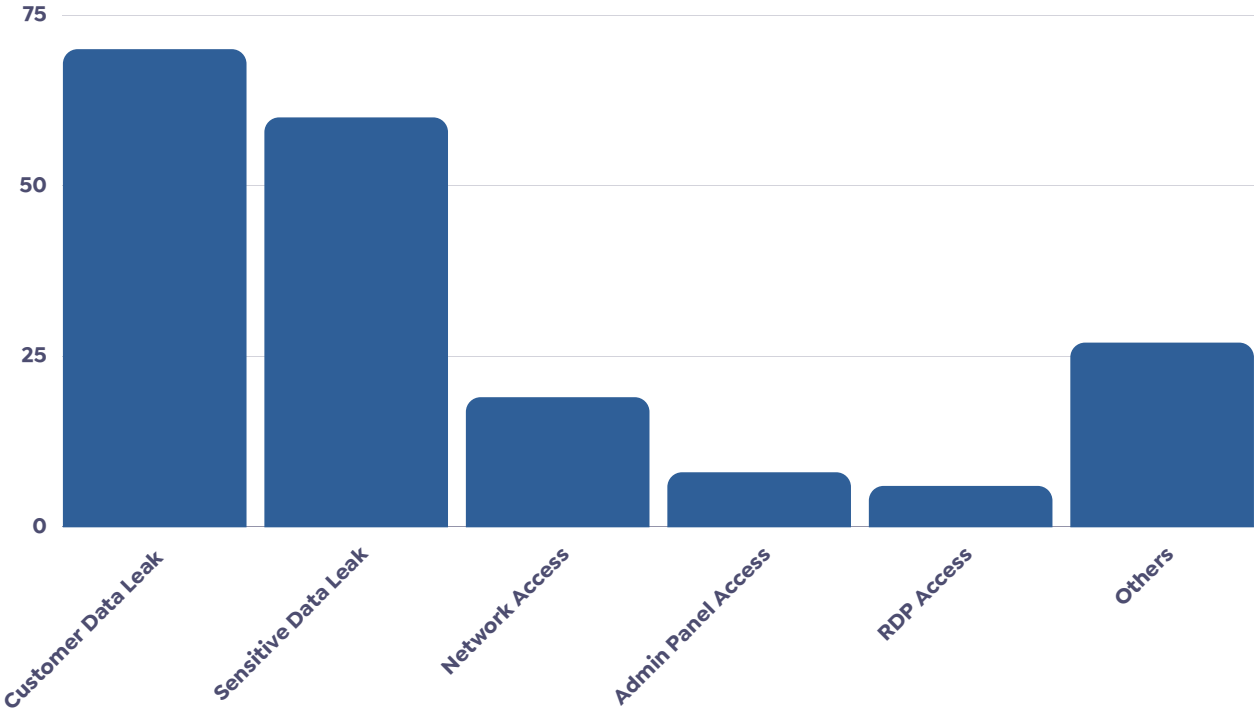
According to DarkMirror data, Thailand's top three most targeted verticals were the "public sector, education, and media & entertainment" industries.

Dark Web Threats: Top 5 Verticals



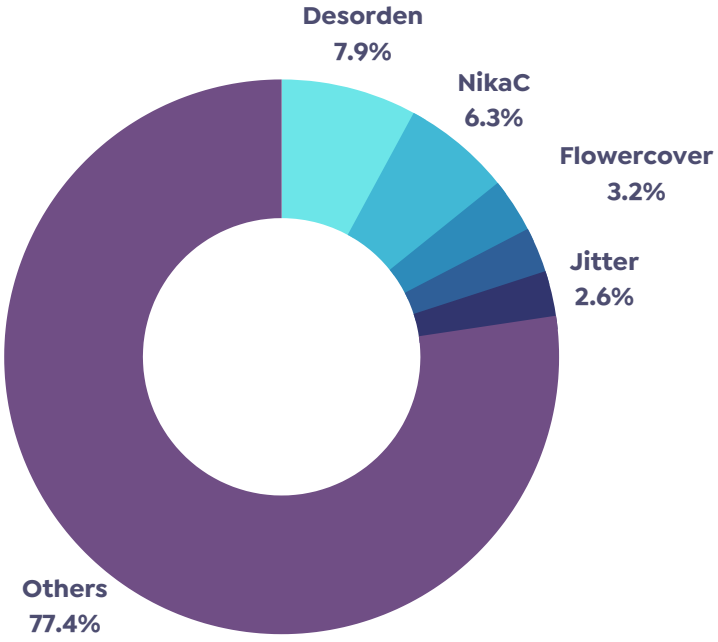
According to SOCRadar's analysis, "more than half of the dark web posts" were customer data leak posts. This means that threat actors leaked customer PII from Thai organizations or sensitive data leak posts where threat actors leaked sensitive information from company data. In sensitive data leak posts, the exposed data includes private companies and government agencies' confidential data, employee PIIs and much more.

Dark Web Threats: Top 5 Dark Web Post Types

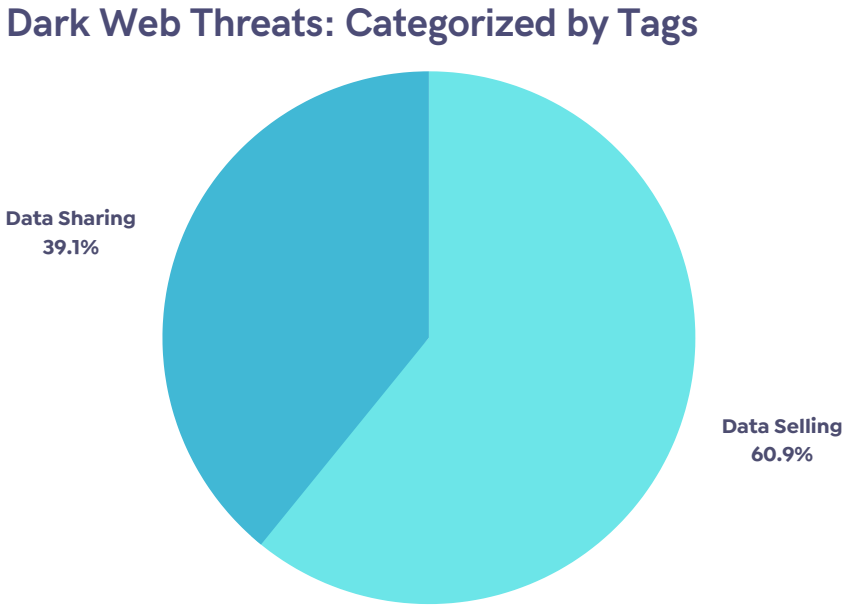


According to SOCRadar's analysis, 121 unique threat actors targeted Thailand in our period. Below, you can see the most active threat actors targeting Thai organizations.

Dark Web Threats: Most Active Threat Actors



The price for the database is sometimes determined through an auction, but in some cases, the price is fixed. In the last 12 months, of all 190 dark web posts targeting Thai organizations, about 60 percent were data-selling posts.

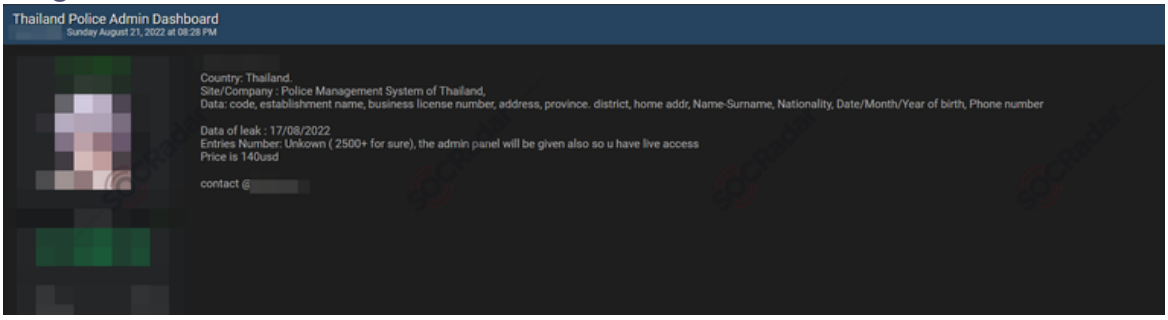


Major Dark Web Incidents

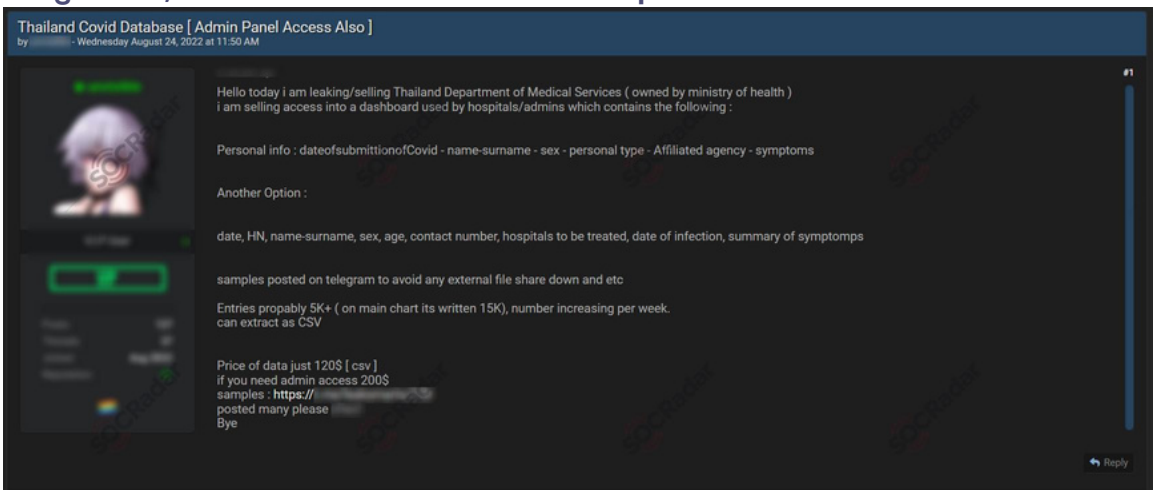
In the dark web posts that the SOCRadar platform constantly monitors, most Thai-related ones were for the "public sector." However, there were no attacks on the private sector either. A recent example of this occurred on 18 February 2022, when a private telecommunications company that provides mobile services in Thailand was hacked. This caused the information of approximately 100,000 users to be leaked onto the dark web.

(September 1, 2022) Database of Ministry of Education Thailand is on Sale

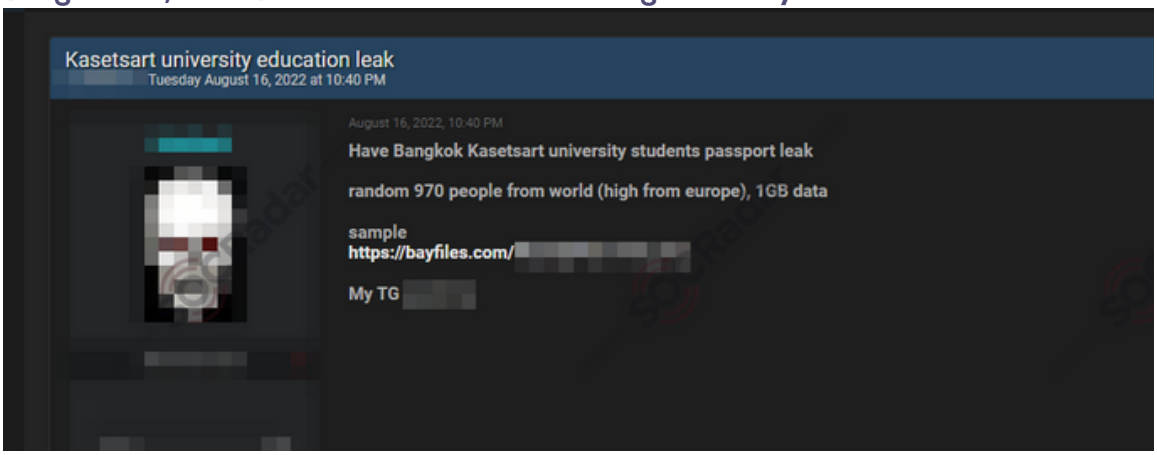
(August 26, 2022) Thailand Covid Database is on Sale



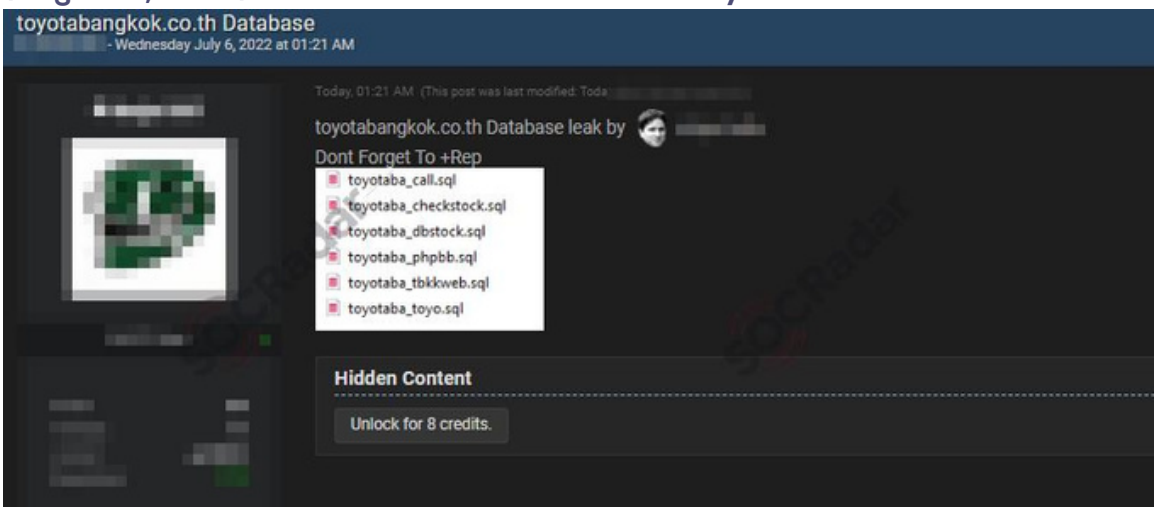
(August 24, 2022) Database of Thailand Department of Medical Services is on Sale



(August 21, 2022) Database of Police Management System of Thailand is on Sale

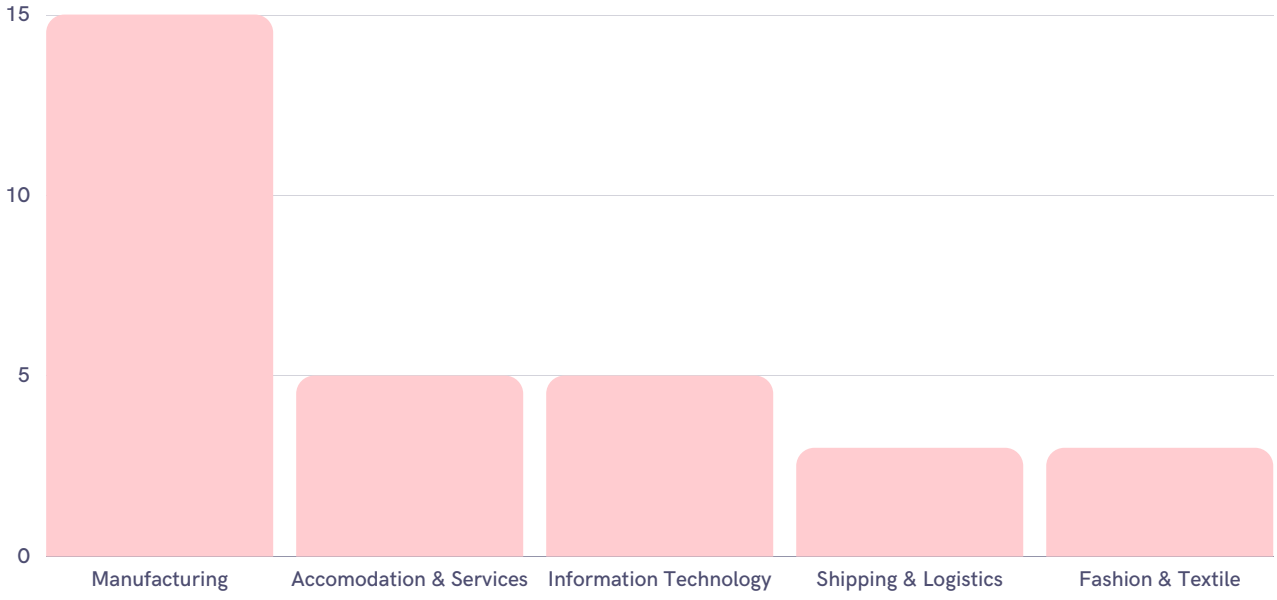


(August 8, 2022) Database of Kasetsart University students is on Sale



Ransomware Threats

Between September 2021 and September 2022, SOCRadar detected 2,900 ransomware incidents globally, targeting 52 distinct ransomware groups. 53 of these incidents belonged to organizations in Thailand. About one-third of all ransomware attacks targeted companies in the manufacturing industry. Below, you can see the top 5 most targeted verticals in ransomware attacks in Thailand.



Top Ransomware Groups Targeting Thai Organizations

SOCRadar monitored 20 unique ransomware groups targeting Thai businesses during the scope of this report. The LockBit group was responsible for nearly half of all ransomware attacks against Thailand. The top 3 most active ransomware groups are the LockBit 3.0, Conti, and AlphVM Blackcat.

LockBit 3.0

- Ransomware-as-a-service (RaaS) operator.
- Has one of the best-designed locker algorithms regarding encryption speed and overall functionality.
- As of late June 2022, the gang declared that a new version of their locker is out: LockBit 3.0. LockBit 3.0 has more outstanding capabilities and functionalities than the old locker. The latest version can be considered a massive threat to organizations worldwide, and we see that the group has started using its new locker.

Conti

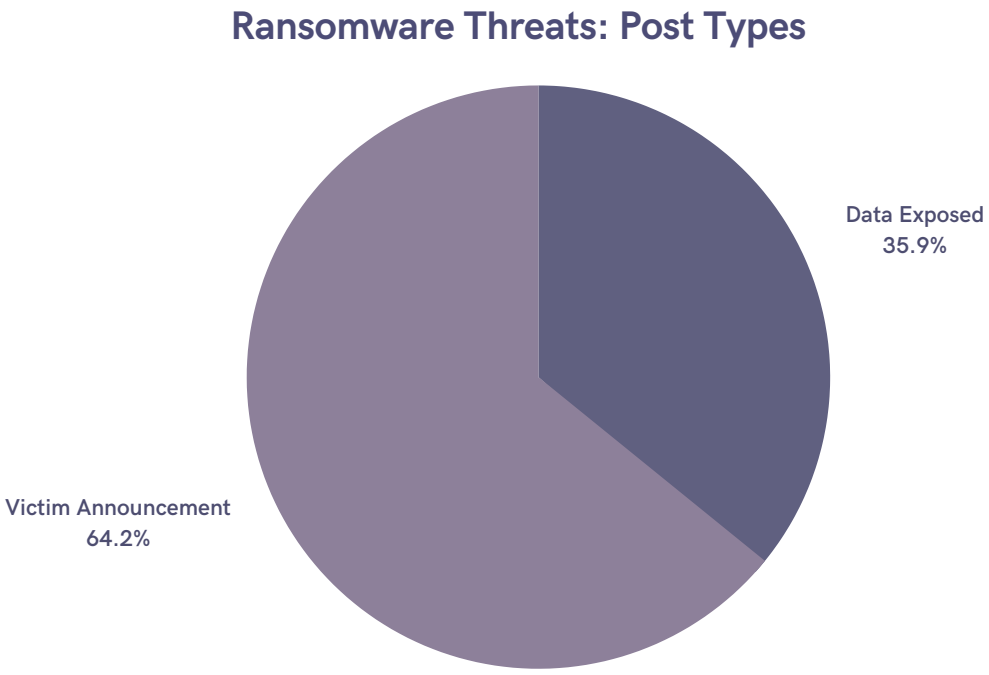
- Ransomware-as-a-service (RaaS) operator, believed to be originated in Russia.
- Conti was one of the most active ransomware gangs, targeting enterprises worldwide.
- After the gang's stand in the cyber crisis between Russia and Ukraine, their internal chats and locker source code were leaked by a Ukrainian hacker who previously had gained access to Conti's internal systems.
- In May 2022, the group stopped its operations, taking its infrastructure offline. They also declared that the group's affiliates would form new partnerships with other ransomware groups.

AlphVM Blackcat

- The first emerged in November 2021.
- Actively recruits ex-REvil and ex-BlackMatter members.
- Unlike other popular ransomware lockers, the group's locker is written in Rust programming language.

The latest data on ransomware attacks against organizations in Thailand within the data scope of this report is "post type." When a ransomware attack hits an organization, the ransomware group demands a ransom from the victim, threatens to disclose the stolen sensitive data publicly, and announces the victim on dark websites.

If the victim does not comply and refuses to pay the ransom, the group exposes the data stolen in the ransomware attack. Observing the threat actor's data posted on the leak site, we can estimate that 19 out of 53 ransomware victims refused to pay the ransom.



Credentials & Stolen Data Intelligence

An Infostealer (Redline, Racoon, Vidar, etc.) is a type of malicious software (malware) that is used to steal credentials of login information, e-mail addresses, and passwords. Threat actors utilize this information to obtain money by selling credentials on the dark web. SOCRadar detected the number of users infected with infostealers and the number of leaked credentials on the dark web in Thailand, which are:

- 88,588 Thailand users have been infected with Stealer (Redline, Raccoon, Vidar, etc.).
- 990,910 credentials that access ".th" domains are leaked from the users and distributed on the dark web.

Top 10 Domains Including ".th" are Recorded As:

- lazada.co.th
- shopee.co.th
- exe.in.th
- rd.go.th
- ku.ac.th
- gg.in.th
- trueinternet.co.th
- sso.go.t
- winner.co.th
- dbd.go.th

DDoS Attacks

Between September 2021 and September 2022, 24 different DDoS attacks were recorded against Thailand with a duration of at least one hour. Most DDoS attack targets are networked companies and internet service providers.

Recursion Enabled Devices

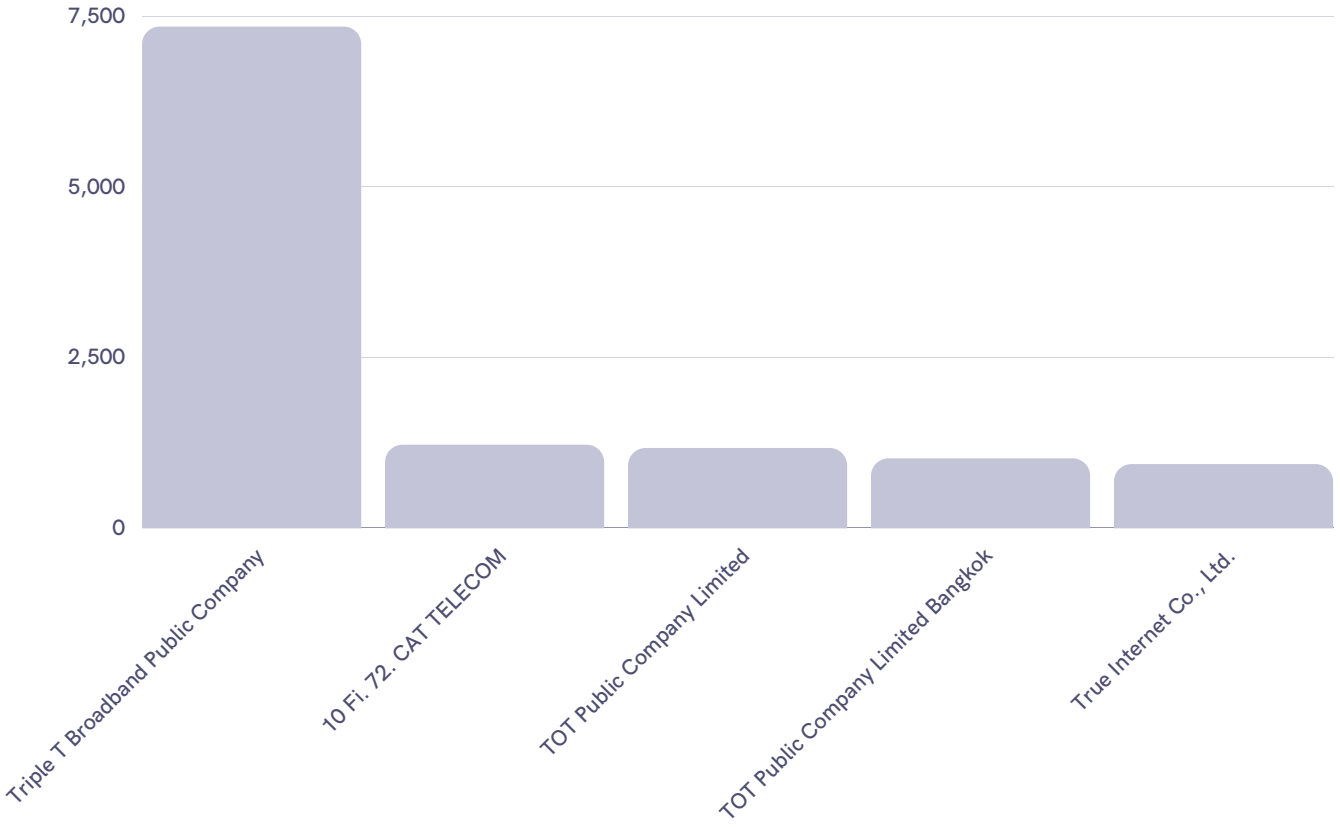
Recursive and iterative requests are the two main forms of DNS queries used to communicate with a server. Recursive requests cause your server to try to locate the requested webpage in its local cache. It will make additional inquiries if it cannot respond until it locates the address. The outcome of each inquiry will then be returned in response to the first request.

Recursive DNS requests are not advised since the servers that accept this type of request are open to queries from a faked IP address, which can become overloaded by the volume of DNS inquiries it receives and become unable to handle legitimate Internet traffic.
42,913 recursion-enabled devices have been detected in Thailand within the specified time scope.

The statistical data of these recursion-enabled devices from Thailand are as follows:

Top Cities

Top Organizations



State Sponsored APT Activities

Advanced Persistent Threat groups (APT groups) are groups of threat actors generally sponsored by governments to carry out the government's malicious activities. APT groups are not financially motivated. Their nation's requests determine their goals. Most APT groups targeting Thai organizations are believed to be of Chinese origin.

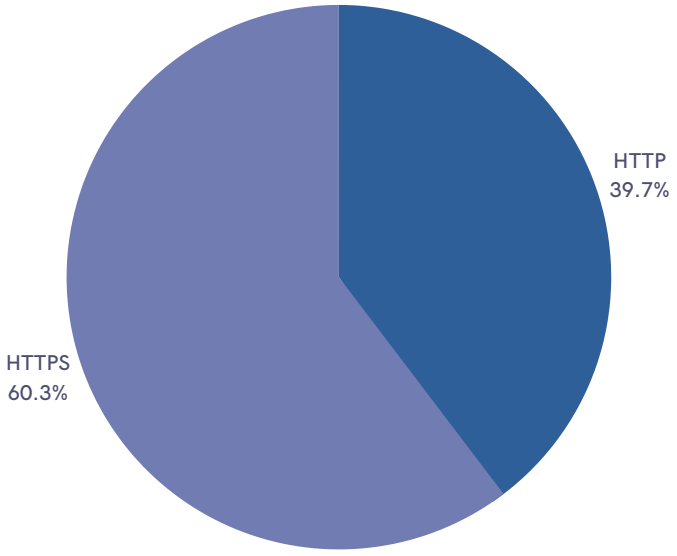
Significant APT Groups

- Lazarus Group
- Axiom
- Naikon
- EMISSARY PANDA
- Earth Lusca
- Stone Panda
- ToddyCat

Phishing Attacks

SOCRadar observed 590 phishing attacks targeting companies in Thailand within the time scope of this report. About 60 % of these phishing websites were hosted on HTTPS domains using a valid SSL certificate.

Phishing Threats: Categorized by SSL Protocol



More than half of the phishing websites were hosted on HTTPS domains using a valid SSL certificate shows us that the threat actors are increasingly using HTTPS to trick users into falling into their phishing traps. Tactics and methods the threat actors use to realize their malicious intent are getting increasingly complex daily.

Critical Asset Exposure and Vulnerabilities

"Critical Asset Exposure" and "Attack Surface Management" solutions are essential features of a company's overall security solutions. Implementing robust ASM solutions enables companies to defend themselves proactively against critical cyber-attacks.

As of 24th September 2022, Thailand had more than 3 million open ports. Approximately 17,000 open ports were open Remote Desktop Protocol (RDP, port 3389) ports. Threat actors could launch dictionary attacks or brute force attacks and remotely access a company's infrastructure through open RDP ports. SOCRadar recommends that organizations in Thailand must disable unused open RDP ports to prevent potential breaches.

Port 7547: 766,326	Protocol: TCP Service: tr069
Port 80: 442,724	Protocol: TCP Service: HTTP
Port 443: 356,841	Protocol: TCP Service: HTTPS
Port 161: 126,567	Protocol: TCP/UDP Service: SNMP
Port 123: 92,211	Protocol: UDP Service: NTP
Port 22: 83,912	Protocol: TCP/UDP/SCTP service: SSH
Port 53: 73,341	Protocol: TCP/UDP Service: DNS
Port 2000: 47,565	Protocol: TCP Service: Callbook
Port 8008: 44,211	Protocol: TCP Service: Fortinet
Port 554: 39,062	Protocol: TCP Service: RTSP

For example, even though the following vulnerabilities were patched for a long time, 2880 hosts were vulnerable to the HeartBleed vulnerability (CVE-2014-0160), and 1050 hosts were vulnerable to the BlueKeep vulnerability (CVE-2019-0708). In addition to these patched vulnerabilities, we see many other (some patched, some unpatched) vulnerabilities in open ports in Thailand.

Critical vulnerabilities and the number of vulnerable hosts in Thailand

	Vulnerable Hosts	CVE ID	CVSSv3
45,279	Improper Initialization	CVE-2022-22719	CVSS: 7.5
45,279	HTTP Request Smuggling	CVE-2022-22720	CVSS: 9.8
45,279	Integer Overflow or Wraparound	CVE-2022-22721	CVSS: 9.8
44,936	Allocation of Resources Without Limits or Throttling	CVE-2022-30522	CVSS: 7.5
44,488	Integer Overflow or Wraparound	CVE-2022-28615	CVSS: 9.1
44,350	Allocation of Resources Without Limits or Throttling	CVE-2022-29404	CVSS: 7.5
44,047	Out-of-bounds Write	CVE-2022-30556	CVSS: 7.5

Our Recommendations

Cyber attacks are not a matter of "if "but "when" for financial firms.

1. Keeping Track of the Vulnerabilities of Digital Assets

There are specific vulnerabilities and zero days that threat actors love to exploit. SOCRadar discovers almost all your digital assets and their vulnerabilities. SOCRadar's External Attack Surface Mapper tracks and updates your assets and vulnerabilities.

2. Identifying and Monitoring Threat Actors

Many organized threat actors like APTs have signature Tactics, Techniques, and Procedures (TTPs). Some of them are only actives and specific regions and sectors. Monitoring the threat landscape and threat actors will make your defenses stronger. SOCRadar's threat intelligence threat feeds, IOCs and IOAs will give you the proactive readiness you need.

3. Phishing Control

Social engineering and phishing are the starting vectors for many cyber attacks. In addition to your company's training for not untrusted links and e-mail attachments without verifying their authenticity, SOCRadar can discover impersonating and typo-squatting domains that could be used for phishing campaigns against your customers and employees.

4. Dark Web Awareness

Threat actors often find their way into systems by purchasing credentials or intelligence from dark web forums and chatter channels. SOCRadar monitors these channels and creates alarms and incidents for anything related to your company.

In addition to these steps, there are more things to protect yourself, such as:

- Using multiple-factor authentication (MFA) and one-time-password (OTP) technologies, you could create strict identity and access management policies.
- You could protect your endpoints using trusted security software as much as possible.
- You must have backup policies and practices. In addition, you should have multiple recent copies (preferably at least one offline) of your critical data and settings and configurations of your security devices.