Singapore: an OSINT-based Threat Intelligence Report (Jan 2024)

Note: This report is based on OSINT data and information retrieved from the following sources and references:

- https://datareportal.com/reports/digital-2023-singapore
- https://www.singstat.gov.sg/
- https://www.businesstimes.com.sg/singapore/smes/singapore-smes-contractionary-mode-full-year-2023-ocbc
- https://cybermap.kaspersky.com
- https://statistics.securelist.com/country/singapore/
- https://www.imperva.com/cyber-threat-attack-map/
- https://malwarefixes.com/
- https://attack.mitre.org/

General Information (as of 2023)

Population: 6 million

Internet Penetration: 5.81 million (96.9% of the overall population)

Social media users: 5.08 million (84.7% of the overall population)

Mobile devices: 9.22 million (153.8 % of the overall population)

288,000 SMEs (99% of all enterprises, employing 71% of the local workforce. ~70% classify as "micro" enterprises), across a variety of sectors including:

- Trade and Retail
- Food & Beverage
- Education
- Business and Financial Services
- Computer and Information Services

Being the main technological and financial hub in Southeast Asia, Singapore is a natural target for cyber attacks across all sectors. Recent notable incidents in the past few years include the MINDEF and the SingHealth data breaches in 2017 and 2018 respectively (see https://www.fca.edu.sg/blog/top-major-cyber-attacks-in-singapore/)

Key Findings

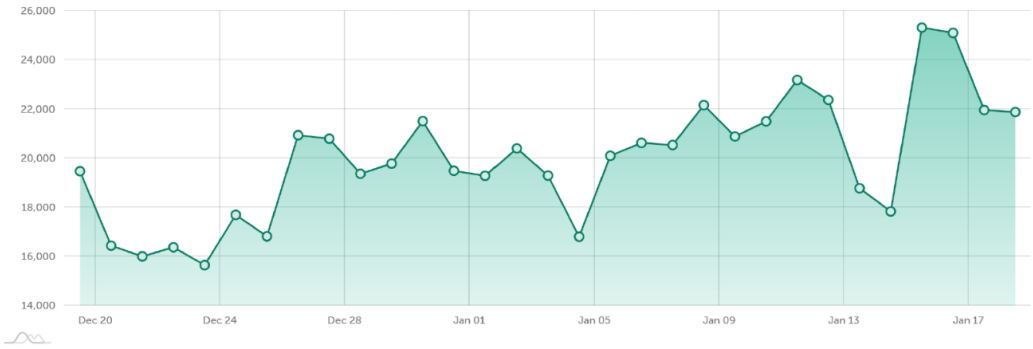
- During the timeframe under analysis, i.e. in the period between mid-December 2023 to mid-January 2024, Kaspersky regularly ranked Singapore within the top #30 most attacked countries in the world and data from Imperva showed more than 57 million attacks in a single day.
- Most targeted sectors are:
    - Financial Services (by far the most exposed sector, targeted by 68.6% of overall attacks)
    - Travel (19.6%)

  - Retail (1.1%)
  - Education (0.7%)
  - Other Businesses (9.8%)`
- Data from Imperva also shows that the most common attacks are based on:
  - OWASP (74.7%) (https://owasp.org/www-project-top-ten/)
  - Automated Threats (23.67)
  - DDOS (2.8%)
- 63% of attacks are originating within the country itself, followed by China (9.6%) and the USA (7.2%) (Source: Imperva).
- These data show that Singapore-based users and businesses are very much a potential target for criminal operations and are under constant pressure. Nonetheless, Kaspersky's "On Access Scan" (OAS) and "On Demand Scan" (ODS) data show a relative low number of actual infections, ranking Singapore only as #154 and #172 in the world respectively. Thus, indicating a highly resilient and well protected infrastructure.

Analysis

The high prevalence of OWASP based attacks as well as automated (tool based) attacks indicates that websites and internet-exposed networks are constantly under pressure.

For web related vulnerabilities, the detected attacks were all trying to either force some form of trojan into the targeted systems or to make users fall into some form of phishing trap (see Figure 1).



1	Trojan.Script.Generic	51,83%
2	Trojan.JS.Agent.gen	17,14%
3	Hoax.HTML.Phish.abf	11,47%
4	Hoax.HTML.Phish.gen	10,47%
5	Trojan.Script.Agent.gen	2,85%
6	Trojan-PSW.Script.Generic	1,72%
7	Trojan.Win32.Bublik.pef	0,72%
8	Trojan-Clicker.Script.Generic	0,52%
9	Hoax.Script.Scaremail.gen	0,48%
10	Trojan.Script.Miner.gen	0,45%

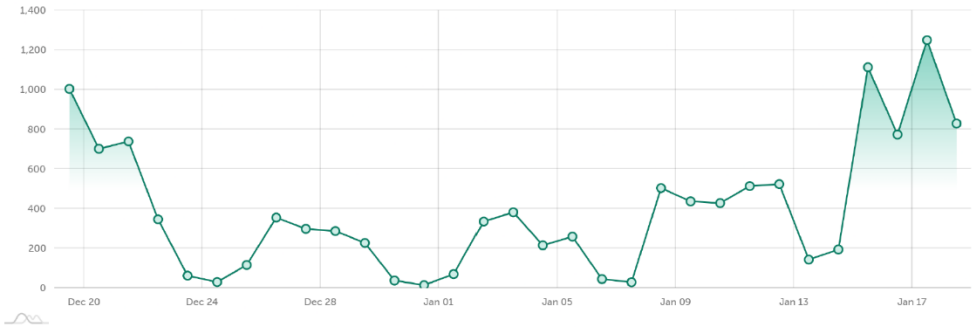
Figure 1: Web threats detected in Singapore from December 19th 2023 to January 18th 2024 and corresponding malware (Source: Kaspersky)

Here, in fact, besides the adoption of generic trojans to infiltrate the target systems, we see also a significant presence of "**Hoax.HTML.Phish**" (~22% of incidents), which identifies harmful websites or files engaged in online scams, such as phishing, deceptive virus scans, fraudulent software updates, and illicit traffic referral schemes. Typically, cybercriminals employ this threat to deceive computer users into visiting a website, posing a risk to their online privacy and security.

The other Trojans detected can bring in a wide variety of threats and can have different capabilities, essentially spanning several of the possible tactics categorized in the **MITRE ATT&CK** framework. For example:

- TA0002: Execution (e.g. T1204.002 User Execution: Malicious File)
- TA0003: Persistence (e.g. T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder)
- TA0004: Privilege Escalation (e.g. T1055.002 Process Injection: Portable Executable Injection and/or T1134 Access Token Manipulation)
- TA0005: Defense Evasion (e.g. T1036.007 Masquerading: Double File Extension and/or T1070.006 Indicator Removal: Timestomp)
- TA0006: Credential Access (e.g. T1003.001 OS Credential Dumping: LSASS Memory)
- TA0007: Discovery (e.g. T1057 Process Discovery, T1082 System Information Discovery, and T1518 Software Discovery)
- TA0009: Collection (e.g. T1115 Clipboard Data)
- TA0011: Command and Control (e.g. T1568 Dynamic Resolution)
- TA0040: Impact (e.g. T1529 System Shutdown/Reboot)

For trojans delivered directly via email, instead, the most common threat reported is the **"Trojan-PSW.MSIL.Agensla.gen**" (PSW: "Password Stealers", MSIL: "Microsoft Intermediate Language"), included in almost 11% of attacks, as shown in figure 2.



1	Trojan-PSW.MSIL.Agensla.gen	10,99%
2	Trojan.Win32.ISO.gen	9,20%
3	Trojan.Script.Generic	8,91%
4	DangerousObject.Multi.Generic	6,51%
5	Hoax.HTML.Phish.gen	6,51%
6	Trojan.Win32.Badun.gen	6,33%
7	Trojan.OLE2.UrcBadur.gen	5,93%
8	Hoax.Script.Scaremail.gen	5,11%
9	Exploit.MSOffice.CVE-2018-0802.gen	3,34%
10	Trojan-Downloader.MSIL.Seraph.gen	2,67%

Figure 2: Email-based attacks and relative malware (Source: Kaspersky).

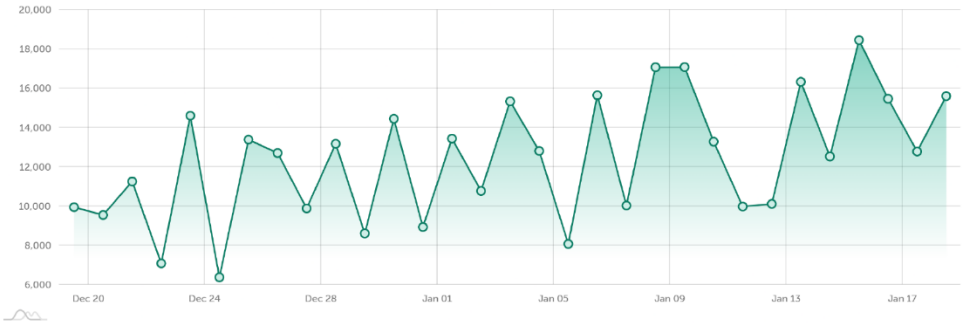
This, as well as similar trojans, target Windows users and aim at retrieving and exfiltrating passwords and other sensitive information. Potentially, though, they have a wide range of capabilities including, for example:

- TA0002: Execution (e.g. T1059.005 Command and Scripting Interpreter: Visual Basic)
- TA0003: Persistence (e.g. T1543.003 Create or Modify System Process: Windows Service, T1555 Credentials from Password Stores)
- TA0004: Privilege Escalation (e.g. T1055 Process Injection, T1543.003 Create or Modify System Process: Windows Service)
- TA0005: Defense Evasion (e.g. T1070 Indicator Removal, T1222.001 File and Directory Permissions Modification: Windows File and Directory Permissions Modification, T1564.003 Hide Artifacts: Hidden Window)
- TA0007: Discovery (e.g. T1087.001 Account Discovery: Local Account, T1518 Software Discovery)
- TA0009: Collection (e.g. T1113 Screen Capture)
- TA0011: Command and Control (e.g. T1071 Application Layer Protocol, T1105 Ingress Tool Transfer)
- TA0040: Impact (e.g. T1499.004 Endpoint Denial of Service: Application or System Exploitation)

Other detected trojans target the Win32 systems by either distributing malicious files as ISO images (**Trojan.Win32.ISO**) or in archives mimicking document files (**Trojan.Win32.Badun**). MS Office is often exploited via the **Exploit.MSOffice.CVE-2018-0802.gen**, which targets the equation editor in Microsoft Office up to the 2016 edition. This exploit allows remote code execution and gives adversaries additional techniques across the abovementioned tactics, especially in the areas of privilege escalation (TA0004), defense evasion (TA0005) and discovery (TA0007).

Network Intrusions are very often initiated by trying to bruteforce an **RDP** connection (see Figure 3). RDP ("Remote Desktop Protocol") is a common way for users to connect to another computer over a network. In a Bruteforce.Generic.RDP attack, the assailant systematically tests all possible login/password pairs to discover a valid combination, potentially leading to unauthorized remote access to the targeted host computer.

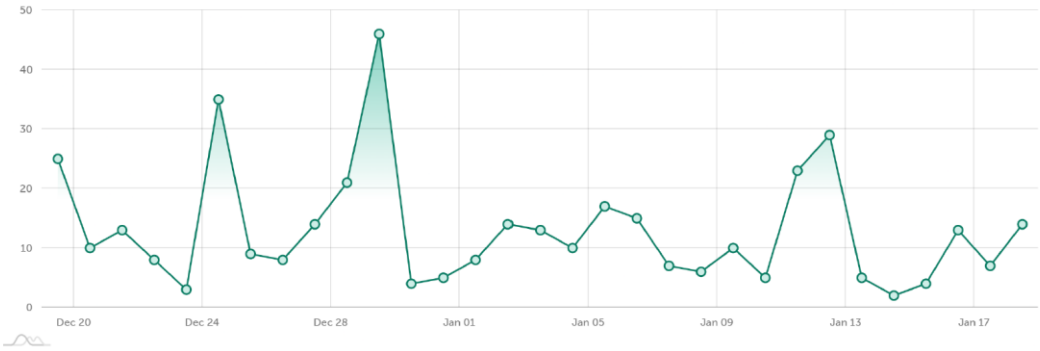
Here we also see that most DDOS attacks happen by means of TCP floods, i.e. by repeatedly sending an initial connection request (SYN) to overload all available ports of the target server, thus making it unavailable to legitimate traffic.



1	Bruteforce.Generic.Rdp.a	37,98%
2	Scan.Generic.PortScan.TCP	29,09%
3	Bruteforce.Generic.Rdp.d	25,51%
4	DoS.Generic.Flood.TCPSYN	5,28%
5	Intrusion.Win.MS17-010.o	1,04%
6	Scan.Generic.PortScan.UDP	0,71%
7	Intrusion.Generic.CVE-2021-44228.a	0,24%
8	Intrusion.Generic.CVE-2018-11776.a.exploit	0,02%
9	Intrusion.Win.MS17-010.p	0,02%
10	Bruteforce.Generic.Rdp.c	0,01%

Figure 3: Network intrusion attempts are mostly done via RDP (Source: Kaspersky).

Last but not least, while the reported incidence of **Ransomware** is relatively low in Singapore, it is still relevant to have a look at what are the most common threats in this area (figure 4):



1	Trojan-Ransom.MSIL.Blocker.gen	17,87%
2	trojan-ransom.win32.Crypren.gen	12,66%
3	Trojan-Ransom.Win32.Blocker.jjgl	9,18%
4	Trojan-Ransom.Win32.Stop.gen	8,19%
5	Trojan-Ransom.Win32.Gen.vho	5,71%
6	Trojan-Ransom.Win32.Vega.a	4,96%
7	trojan-ransom.win32.Crypmod.gen	3,97%
8	Trojan-Ransom.Win32.Convagent.gen	2,98%
9	Trojan-Ransom.Win32.Blocker.pef	2,73%
10	Trojan-Ransom.Win32.Blocker.gfeq	2,48%

Figure 4: Daily ransomware attacks detected in Singapore (source: Kaspersky)

Here, the most common threats are represented by the **Trojan-Ransom.MSIL.Blocker.gen** (17.87%), followed by **Trojan-Ransom.Win32.Crypren.gen** (12.66%). The former is a type of ransomware that prevents the operating system from loading normally and instead of showing the usual welcome screen prompts the user to contact the attacker via SMS for further instructions. The latter, instead, is commonly referred to as the "Cryptowall Trojan" and is particularly dangerous as it spreads across spam messages.

These ransomware infections have very advanced and disruptive capabilities, including:

- TA0002: Execution (e.g. T1129 Shared Modules, T1204.002 User Execution: Malicious File)
- TA0003: Persistence (e.g. T1543.003 Create or Modify System Process: Windows Service, T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder)
- TA0004: Privilege Escalation (e.g. T1134.001 Access Token Manipulation: Token Impersonation/Theft, T1134.002 Access Token Manipulation: Create Process with Token)
- TA0005: Defense Evasion (e.g. T1070.004 Indicator Removal: File Deletion, T1070.006 Indicator Removal: Timestomp,T1112 Modify Registry, T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control)
- TA0006: Credential Access (e.g. T1056.001 Input Capture: Keylogging)
- TA0007: Discovery (e.g. T1082 System Information Discovery, T1083 File and Directory Discovery, T1087.001 Account Discovery: Local Account, T1518.001 Software Discovery: Security Software Discovery)
- TA0009: Collection (e.g. T1115 Clipboard Data, T1560.001 Archive Collected Data: Archive via Utility)
- TA0011: Command and Control (e.g. T1571 Non-Standard Port)
- TA0040: Impact (e.g. T1490 Inhibit System Recovery, T1491.001 Defacement: Internal Defacement)

Recommendations

The main issue exposed by this report is the prevalence of **RDP** based attacks and intrusions (63.5% overall, see figure 2). To mitigate these, the following strategies are recommended if not already in place:

- **Implement Account Lockout Policies:** Configure account lockout policies to automatically lock user accounts after a certain number of failed login attempts.
- **Enable Network Level Authentication (NLA):** Network Level Authentication requires users to authenticate themselves before establishing an RDP session, adding an extra layer of security. NLA needs to be enabled on all RDP servers and client machines in the environment.
- **Use Strong Password Policies:** Enforce strong password policies for RDP accounts, requiring complex passwords that include a mix of uppercase and lowercase letters, numbers, and special characters. Passphrases are recommended as well as implementing multi-factor authentication (MFA) for an additional layer.
- **Change Default RDP Port:** Changing the default RDP port (TCP port 3389) can help deter automated attacks that specifically target this port. By using a non-standard port, a system administrator can make it more challenging for attackers to discover and exploit the RDP service.

- **Implement Rate Limiting:** Implement rate-limiting mechanisms to restrict the number of connection attempts within a specific timeframe. This helps mitigate brute-force attacks by slowing down attackers' ability to make multiple login attempts rapidly. Firewalls or intrusion detection/prevention systems should be used to enforce rate-limiting policies at the network level.

As exploiting RDP connections is a common attack vector, it is also highly recommended to constantly **Monitor and Audit** the ongoing RDP activity to track login attempts, including successful and failed connections, to promptly identify any suspicious behavior.

While **DDOS** attacks may not seem particularly serious at this time and appropriate measures seem to be already in place, the ongoing presence of TCP SYN flood attacks should still be addressed. Mitigating these requires a combination of network and system-level strategies to help prevent overwhelming the targeted systems, including:

- **Implement Rate Limiting**: Use rate limiting to control the rate of incoming TCP SYN packets. By setting reasonable thresholds for connection requests, excessive connection attempts can be identified and blocked, mitigating the impact of the flood.
- **TCP SYN Cookies:** Enable TCP SYN cookies on the servers. This technique allows a server to continue accepting new connections during a SYN flood by encoding the initial sequence number in the SYN-ACK response. It helps mitigate the impact of incomplete connection attempts (https://en.wikipedia.org/wiki/SYN_cookies).
- **Firewall Configuration:** Review and finetune the firewall configuration to identify and filter out malicious traffic associated with the TCP SYN flood. Specific rules can be added to block or limit traffic from suspicious IP addresses and stateful inspection can be implemented to monitor the state of incoming connections.
- **Load Balancers**: Distribute incoming traffic across multiple servers using load balancers. This helps spread the impact of a TCP SYN flood across several servers, making it more difficult for the attacker to overwhelm any single system.
- **Anomaly-Based Detection Systems:** Deploy intrusion detection and prevention systems that use anomaly-based detection to identify abnormal traffic patterns indicative of a possible incoming TCP SYN flood. These systems can automatically trigger protective measures when unusual behavior is detected.
- **Cloud-based DDoS Protection Services:** Cloud-based DDoS protection services that specialize in mitigating large-scale attacks can also help. These services have the infrastructure and expertise to absorb and filter malicious traffic, preventing it from reaching the targeted network.

Besides these technical measures, it is also important to have a proper Incident Response Plan (IRP) and a relative playbook specifically tailored for DDoS attacks, including TCP SYN floods. Having predefined steps and communication procedures can help minimize downtime and reduce impact.

Conclusions

To conclude, the prevalence of OWASP and automated attacks seem to indicate that threat actors are financially motivated black hat hackers/criminals who are trying to target as many different businesses as possible by following standard procedures and approaches, hoping to find a vulnerable target to take advantage of.

Since the actual rate of infections is relatively low, as reported by the OAS and ODS data reported by Kaspersky, it seems that most of the local IT infrastructure in Singapore is well protected against this kind of threats, with local business and organizations of all sizes showcasing high awareness of common best practices in the field, i.e. the importance of patching and updating systems and software regularly. This is also confirmed by the low impact of the Eternal Blue (MS17-010) and Log4j (CVE-2021-44228) vulnerabilities that are still very critical in other countries but, in Singapore, only represent 1.06% and 0.24% of network attacks respectively (figure 3). It is also worth noting that many potential network Intrusions (~30%) are already detected and addressed at the reconnaissance level via the careful monitoring of active scanning (an action that is already considered a crime under Singapore Law if performed without explicit permission), showing a highly effective and proactive approach to cybersecurity by Singaporean businesses.