TLP: AMBER

Sharing on Cyber Threat Landscape

Cyber Security Agency of Singapore

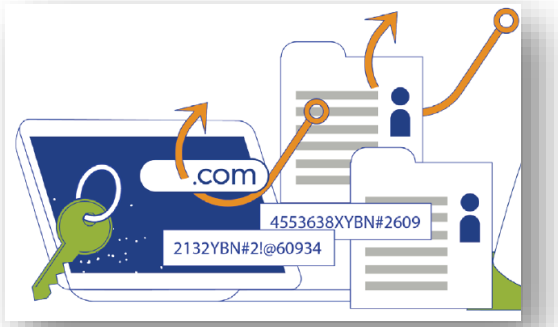
20 November 2024

Scope

1. Local cybersecurity trends
2. Case studies
3. What can we do?

CSA monitors four key malicious cyber activities to gauge the overall cyber hygiene level of Singapore

(but we'll just look at two of them today)



Phishing Attempts

Ransomware Cases

Infected Infrastructure

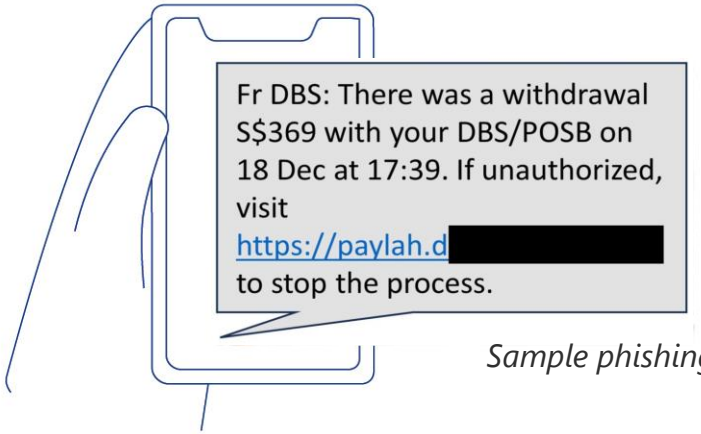
Website Defacements

Phishing Attempts

Most spoofed industries:

1) **Banking and Financial Services**
2) **Government**
3) **E-commerce**

- Banking and Financial Services remained the most spoofed (53% of all phishing attempts impersonate organisations from this industry).



Sample phishing SMS spoofing DBS

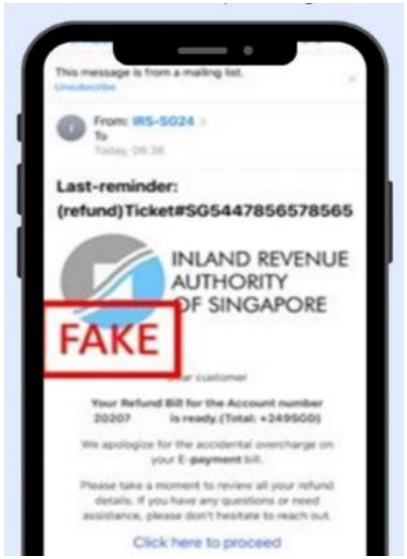
- The most spoofed government agencies were the Ministry of Finance (MOF), Singapore Police Force (SPF), and the Ministry of Manpower (MOM).

- Around one-third of phishing attempts spoofing the Government were aimed at MOF, using the Singapore Budget as the lure.

Phishing Attempts

- From our analysis of reported phishing attempts in 2023, cybercriminals may be shifting tactics to make their phishing attempts more legitimate and authentic, such as an increased use of the:
    a) "HTTPS" protocol, which add credibility to phishing URLs; and
    b) ".com" top-level domain, which is more commonly associated with legitimate brands.

- Threat actors also adjust their lures frequently to capitalise on current events, or reuse effective lures from the past to increase phishing success.



Sample phishing site and email spoofing NTUC FairPrice and IRAS respectively

- Continued vigilance remains key, thus CSA and the Singapore Police Force have been regularly publishing alerts on scam variants.

Phishing is challenging to eliminate since it preys on a range of human emotions...

OUTRAGE

"IS THE GOVERNMENT TELLING US THE TRUTH ABOUT HOW MANY INFECTED???

You will learn these things at this link. Life saving information

ANXIETY

"Do you realize that once one of your family members gets it all of you will be separated?"

Take the pandemic quiz to see if you're prepared.

FOMO

"CLAIM YOUR CORONOVIRUS SURVIVOR CASH REWARD OF $500,000"

Please, in other to claim your Coronavirus Relief Funds of $USD500,000, kindly send your full name and current address by email to [redacted]

CURIOSITY

"Here is the list of updated no. [sic] of Corona Virus Cases confirmed near you"

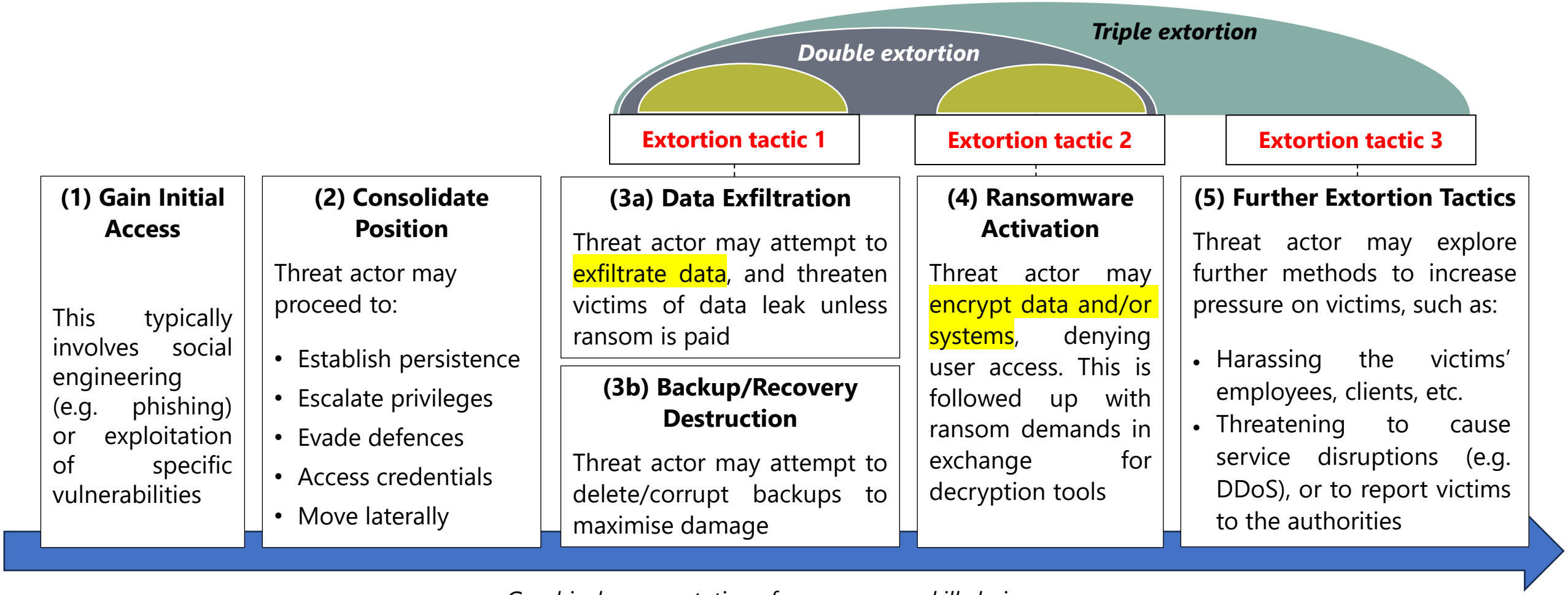
COVID-19 LIST

Ransomware Cases

- There was an average of 1 reported ransomware case locally every 3 days in 2023, contrasted against the global average of 1 reported ransomware case every 2 hours.
- There has been a slight increase in ransomware cases locally in 1H 2024, as compared to 2H 2023.
- Most affected industries include: Professional Services, Manufacturing, and Info-comms Technology (ICT) & Media.

Ransomware is a growing problem for all digitally connected countries

Threat actors constantly evolve their tactics to improve their success in extorting payments from victims



Graphical representation of a ransomware kill chain

Ransomware Case Study: Attack on Local Company (*ZTK Engineering**)

Company Profile

- SG-based manufacturing SME
- >130 employees
- Manufacturing and trade of construction materials
- IT security function handled by company's sole IT manager

Suffered a Ransomware Attack in Jan 2023

- Clients' database, vital business records encrypted
- Major loss of productivity for one month
- Did not pay ransom, but also did not hire IR, did not report to authorities
- Rebuilt systems from scratch
- Suspected that emails were exfiltrated and warned some of its customers
- Potential intrusion vector: Outdated software and lax security practices

**Details anonymised*

Ransomware Case Study: Attack on Local Company (*ZTK Engineering**)

ZTK received an enticing offer from a regular trading partner, *Goodluck Machinery*:

To: Zachary Neo <Zachary.neo@ztk.com.sg>
From: Goodluck Sales <sales@goodlluck_machinery.co.uk>
Cc: Low ZTK <lowztk@ztk.com.sg.

RE: Discounted steel plate clearance

Dear Zac and Low,
How are you? Today's your lucky day. We just conducted a stocktake and want to clear out some surplus steel plates. Would like to offer you 80 pieces ¾ inch at half price. We are feeling generous, so I'd even throw in shipping for free. Am a little strapped for cash now, so we need full payment upfront this time. Let me know if you are keen.

Regards,
Greg

Ransomware Case Study: Attack on Local Company (*ZTK Engineering**)

You'd Guessed Right: It was a SCAM

Missed Signs of Scam

- Spoofed email address
- Unfamiliar bank account
- Failed to verify abnormal deal with partner

What Likely Happened

- Ransomware hackers likely exfiltrated *ZTK's* emails
- They combed through the firm's correspondences, to understand *ZTK's* business dealings
- With this knowledge, they then spoofed one of *ZTK's* trusted partners

Ransomware Case Study: Attack on Local Company (*ZTK Engineering**)

What Actually Happened (Afterwards)

- ZTK lost about $180,000.
- Immediately contacted the bank to halt the transaction, but it was too late; the money transferred multiple times within an hour.
- CSA found several backdoors installed by the hackers to maintain access to *ZTK's* systems. These were swiftly quarantined and purged from the network.
- *ZTK* should have reported the incident and determined the actual impact of the ransomware incident.

No industry is immune to cyber-attacks

- The chemical industry faces potentially more severe consequences if hit by cyber-attacks, given the cyber-physical impact (e.g. chemical releases or explosions). *Thankfully, such incidents remain less common.*

- Besides threat actors enhancing their sophistication, the chemical industry may face greater cybersecurity risks due to increased connectivity and/or adoption of new technologies (e.g. to facilitate remote troubleshooting or for automation purposes). These can inadvertently create new entry points or vectors that can be exploited by attackers.

- Some examples of significant cyber-attacks impacting the chemical industry include:

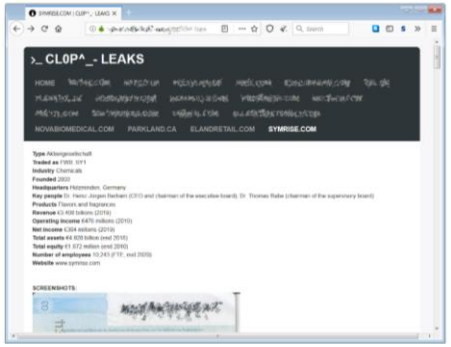

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

Share full article

Colonial Pipeline ransomware attack (2021)

- Pipelines were shut down after the company's IT systems were hacked (to prevent the malware from spreading).
- Incident caused widespread disruption to US fuel supplies. Colonial Pipeline also suffered substantial loss of income, reputational damage, and legal ramifications.



Symrise's data posted on a data leak site

Symrise ransomware attack (2020)

- Symrise was forced to shut down its operations after the attack.
- Close to 1,000 devices in Symrise were encrypted. 500 GB of sensitive data was also exfiltrated, some of which were subsequently leaked by the ransomware group.

- Singapore companies are not spared. More broadly, the manufacturing sector has also consistently ranked among the most impacted by ransomware attacks locally in recent years.

Most threats can be prevented / mitigated with good cyber hygiene practices

Such practices include:

Establish Strict Access Controls

- Identify all digital assets
- Institutionalise controls on admin and remote privileges
- Whitelist applications and devices

Enforce Strong Password Management

- Strong password policy
- Multi-factor Authentication
- Credential management policy

Perform Regular Software Updates

- Update software and firmware promptly
- Use automatic updates where feasible

Regularly Backup Important Data

- Identify important data
- Schedule regular backup and before key events
- Ensure backups are stored offline

Develop Cyber Monitoring & Incident Response

- Establish monitoring and logging capabilities to detect breaches
- Perform regular security assessments on key systems
- Develop and validate incident response plan

Protect Against Social Engineering

- Deploy email filtering and anti-phishing solutions
- Deploy mobile threat defence software, e.g. ScamShield
- Train staff (and oneself) to spot the signs of phishing

Addressing all three pillars of cybersecurity – People, Process, and Technology

Cyber hygiene in previous slide mainly addresses the Process and Technology pillars of cybersecurity. However, People is arguably the most critical.

Security Awareness and Training to Increase Vigilance

- Regularly share articles on the emerging threats, common intrusion vectors and how to spot them
- Perform social engineering simulation exercises to keep staff aware and understand weaknesses
- Raise awareness safeguarding account credentials
- Encourage individual cybersecurity hygiene (even on personal devices)

Clear Communication and Responsibilities

- Roles and responsibilities of all staff need to be established
- Ensure that staff are aware of what to do and who to inform during a cybersecurity incident
- Report near-miss incidents too

THANK YOU

www.csa.gov.sg

CSAsingapore

CSA SINGAPORE