Joint Advisory on ALTDOS

This joint advisory is the result of a collaborative effort between the Cyber Security Agency of Singapore (CSA), the Personal Data Protection Commission (PDPC) and the Singapore Police Force (SPF). Collectively, we have received several reports of cyber incidents involving organisations operating in Singapore that were reportedly targeted by the threat actor ALTDOS.

This joint advisory highlights the observed Tactics, Techniques and Procedures (TTPs) employed by ALTDOS to compromise their victims' networks and provides some recommended measures for organisations to mitigate the threat posed.

Background of ALTDOS

ALTDOS first emerged in late 2020 when they claimed their first victim, a securities trading firm based in Thailand. Thus far, ALTDOS has claimed multiple victims in Bangladesh and Singapore, in addition to Thailand. The threat actor appears to operate primarily in Southeast Asia and Bangladesh, targeting businesses for financial gains.

Observed TTPs employed by ALTDOS

Domain	ID	Name	Use
Enterprise	T1595.002	Active Scanning: Vulnerability Scanning	ALTDOS performs active scanning to identify vulnerable public facing services and web applications
Enterprise	T1588.002	Obtain Capabilities: Tool	ALTDOS leverages third-party penetration testing tools such as Cobalt Strike
Enterprise	T1190	Exploit Public-Facing Application	ALTDOS exploits outdated versions of public-facing web services to gain initial access
Enterprise	T1059	Command and Scripting Interpreter	ALTDOS uses interpreters to execute arbitrary code and establish backdoor access
Enterprise	T1505.003	Server Software Component: Web Shell	ALTDOS deploys web shells in compromised server to execute code and establish persistence
Enterprise	T1068	Exploitation for Privilege Escalation	ALTDOS exploits vulnerabilities in the software for privilege escalation
Enterprise	T1055.003	Process Injection: Thread Execution Hijacking	ALTDOS hijacks legitimate processes to hide the malware
Enterprise	T1095	Non-Application Layer Protocol	ALTDOS establishes communications between C2 and installed malware (usually Cobalt Strike Beacon)
Enterprise	T1486	Data Encrypted for Impact	ALTDOS encrypts compromised system to extract ransom

Enterprise	T1561.001	Disk Wipe: Disk Content Wipe	ALTDOS wipes the contents of the compromised system

Observed TTPs (and associated IDs) employed by ALTDOS mapped to MITRE ATT&CK

ALTDOS typically uses double extortion techniques to extract ransom from their victims. In double extortion, data is exfiltrated from the victim's servers, after which the data may be encrypted. ALTDOS will subsequently contact the victim using an email address hosted on protonmail demanding that payment be made or the exfiltrated data will be published (leak-and-shame). It is currently unknown which ransomware variant is employed by ALTDOS. Victims have also been asked to pay a separate ransom if they wish to decrypt any encrypted files. Similar to other financially motivated threat actors, the ransom is typically paid in Bitcoin. If the victim does not respond or comply to the ransom demand within the given time frame, ALTDOS may also launch a Distributed Denial-of-Service attack on the victim's Internet facing systems to disrupt operational services and to remind them to pay the ransom.

Detection of TTPs

1. Web Server Exploitation

ALTDOS has been observed to exploit vulnerable instances of Apache Web Servers and employ SQL injection against vulnerable targets to obtain initial access. Besides monitoring the logs provided by Web Application Firewalls, incident responders can also examine host process logs for anomalies between parent web server processes and child processes.

Parent processes that should be monitored include those belonging to web servers such as *httpd.exe* and *php-cgi.exe*. Suspicious child processes include those that can be used as command and scripting interpreters such as *powershell.exe*, *cmd.exe* or *wscript.exe*. When intruding into a victim's network, ALTDOS has been observed to exploit the web server where *httpd.exe* spawns *cmd.exe*, enabling arbitrary code execution.

2. Cobalt Strike Beacons

ALTDOS has been observed to primarily employ default Cobalt Strike Beacons that can be readily identified using open source YARA rules. Please see appended links for the YARA rules:

https://github.com/Neo23x0/signature-base/blob/master/yara/apt_cobaltstrike.yar

https://github.com/Neo23x0/signature-base/blob/master/yara/apt_cobaltstrike_evasive.yar

ALTDOS has also been observed to use default Cobalt Strike TLS/SSL certificates. Incident responders investigating suspicious destination IP/Domains can check the certificate for suspicious fields such as those appended:

Common Name	*Major Cobalt Strike (subject)* *Major Cobalt Strike (issuer)*
Organisation Name	*Cobaltstrike (subject)* *Cobaltstrike (subject)*
Organisation Unit	*AdvancedPenTesting (subject)*

	AdvancedPenTesting (issuer)
Locality	*Somewhere (subject)* *Somewhere (issuer)*
State/Province	*Cyberspace (subject)* *Cyberspace (issuer)*
Country	*Earth (subject)* *Earth (issuer)*

Recommended Mitigations

1. Regular Patching

ALTDOS typically exploits vulnerable instances of web servers to gain initial access to an organisation's network. As such, we strongly recommend that organisations regularly update their softwares (e.g. web server application, database application, etc.) to patch known security vulnerabilities. Source code reviews also help to detect web application vulnerabilities. Vulnerabilities include those in the Open Web Application Security Project (OWASP) "Top Ten" list.

2. Regular Log Reviews

ALTDOS has been observed to carry out active scanning to discover vulnerable instances of web servers. As such, system administrators should enable logging (e.g. server access logs) and review such logs regularly to spot any malicious activities (e.g. SQLi attempts). If malicious activities are detected, the originating IP address(es) should be filtered with applicable technologies such as a web application firewall. Affected organisations should also scan their internal corporate networks for any malicious activities.

3. Network Segregation or Segmentation

Organisations using web servers are also encouraged to deploy network segregation or segmentation techniques that limits communications between internet facing services and internal servers such as those containing sensitive data. This will limit the impact of threat actors who may successfully gain initial access to vulnerable web applications and reduce the probability of a data breach.

4. Implement Routine Backups

Organisations should implement routine backups that creates and saves copies of important files to external and offline storage devices. This will allow for system restoration that mitigates the impact of a ransomware incident and minimises data loss. Backup media should be regularly tested to ensure that the backup data can be recovered and restored in time to help the business recover from data corruption or destruction.

5. Employ Web Application Firewalls

Organisations should also employ web application firewalls to filter malicious network traffic (e.g. SQLi) and "harden" their system configurations (e.g. for web server and firewalls) by making appropriate changes to settings and not rely on default settings.

6. Seek External Assistance

Organisations may also wish to hire a professional firm to routinely perform web application penetration testing and vulnerability scanning to identify vulnerabilities that may enable threat actors to gain initial access to their network. Organisations should also seek professional assistance from cybersecurity service providers for incident response and remediation if a cybersecurity incident is confirmed.

Should you pay the ransom?

In the event that your organisation's systems are compromised, we do not recommend paying the ransom and advise you to report the incident to the authorities. Paying the ransom does not guarantee that the data will be decrypted or that your data will not be published by threat actors. It also encourages the threat actors to continue their criminal activities and target more victims. Threat actors may also see your organisation as a soft target and may strike again in the future.

Additional Resources:

SingCERT Ransomware Advisories:

https://www.csa.gov.sg/singcert/Advisories/ad-2021-006
https://www.csa.gov.sg/singcert/Advisories/ad-2020-006

CSA Incident Response Checklist:

https://www.csa.gov.sg/singcert/Resources/Incident-Response-Checklist

PDPC Guides to Protect Against Data Breaches:

https://www.pdpc.gov.sg/Help-and-Resources/2021/05/Guard-Against-Common-Data-Breaches
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf?la=en
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Protection-by-Design-for-ICT-Systems-(310519).pdf?la=en

No More Ransom Initiative:

https://www.nomoreransom.org/

MITRE ATT&CK Framework:

https://attack.mitre.org/matrices/enterprise/

Issued by:

CSA SINGAPORE

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY