JOINT ADVISORY BY THE CYBER SECURITY AGENCY OF SINGAPORE (CSA), SINGAPORE POLICE FORCE AND THE PERSONAL DATA PROTECTION COMMISSION (PDPC) SINGAPORE

JOINT THREAT ADVISORY ON GHOSTR

The Cyber Security Agency of Singapore (CSA), the Singapore Police Force (SPF) and the Personal Data Protection Commission (PDPC) have received several reports from organisations affected by the cyber threat actor GhostR in the last three months. This advisory provides information on observed Tactics, Techniques and Procedures (TTPs) employed by GhostR to compromise their victims' networks and recommends measures for organisations to mitigate the threats. Information from this advisory is drawn from various sources, including but not limited to National CERT publications, open-source information, incident investigations, and threat intelligence reports.

Background of GhostR

GhostR first emerged in August 2023. GhostR is a financially motivated threat actor known for stealing, demanding ransom and selling confidential information belonging to their victims. Thus far, GhostR has claimed multiple victims, with an observed focus on entities in the Southeast Asia region, though organisations in other countries have also been affected (e.g. India).

Observed Tactics, Techniques and Procedures (TTPs)

Technique	ID	Description
Initial Access		
Active Scanning	T1595	GhostR has been observed to employ port scanning or vulnerability scanning tools to identify weaknesses in target systems.
Exploit Public-Facing Application	T1190	GhostR has been observed to exploit vulnerabilities in externally facing applications, like Microsoft Structured Query Language (SQL) Server which could be leveraged to gain initial access.
Valid Accounts	T1078	GhostR has been observed to use legitimate accounts to help them blend in with normal activity and evade detection by security tools.
Persistence		

Create Account	T1136	GhostR has been observed to create new user accounts on the compromised system to establish persistence even after a reboot or change of credentials for affected accounts.
Discovery		
Network Service Discovery	T1046	GhostR has been observed using specific tools to gain knowledge on the victim's system and its connected network, such as the use of sqlmap to gather information about database schema, tables, columns, and other metadata.
Exfiltration and Impact		
Exfiltration Over Alternative Protocol	T1048	GhostR has been observed to employ several methods to exfiltrate sensitive information from their victims. These include the use of legitimate tools such as WinRAR, to split and compress data prior to exfiltration, PSCP (PuTTY Secure Copy Protocol), which is a Secure File Copy Protocol based on SSH.
Data Destruction	T1485	GhostR has been observed to have deleted databases and files from victims' servers.

Recommended Prevention and Mitigation Measures

Organisations are encouraged to implement and monitor the compliance of the following mitigation measures and policies to strengthen their cybersecurity posture and reduce the risks and impact of a cybersecurity incident perpetrated by GhostR.

Update and Patch Regularly

GhostR typically exploits vulnerable instances of web servers or externally facing applications to gain initial access to an organisation's network. Hence, organisations are strongly encouraged to regularly update their software (e.g. web server application, database application, etc.) to patch known security vulnerabilities. Patches should be prioritised based on functions critical to the business. If immediate patching is not possible or feasible, vendor-provided mitigations should be implemented. For applications that have reached end-of-life (EoL), organisations are recommended to migrate to applications that are supported.

Regularly Review User Accounts

Since GhostR has been observed to create new user accounts to establish persistence, system administrators should regularly review user accounts to ensure that the current list of users are accurate. User accounts should be added or removed when employees join or leave the company accordingly. System administrators can enable notification systems for suspicious activities such as creation of user accounts outside of office hours or by non-administrator accounts.

Implement Principle of Least Privileges

Organisations should practise the principle of least privilege or any other applicable established framework when monitoring and validating privilege of users. This is crucial for minimising security risks by allowing users the lowest access necessary to perform their specific job functions.

This limits the potential damage that can be caused by compromised accounts or configuration errors, as users are restricted to the minimum permissions required for their tasks. It also reduces the chances of a threat actor gaining elevated or administrative privileges.

Implement Secure Coding Practices

Source code reviews and regular security testing help to detect web application vulnerabilities. Vulnerabilities include those in the Open Web Application Security Project (OWASP) "Top Ten" list. Implementing input validation or sanitisation also helps to mitigate possible threats such as SQL injection (SQLi) attacks.

Perform Regular Log Reviews

System administrators should enable logging (e.g. server access logs) and review such logs regularly to identify any malicious activities (e.g. SQLi attempts). If malicious activities are detected, the IP address(es) where malicious traffic originates from 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.

Implement Network Segregation or Segmentation

Network segmentation divides a larger network into smaller sub-networks with limited or more easily monitored network traffic between them. Implementing network segmentation would allow organisations to limit direct communications between internet facing services and internal servers

containing sensitive data, preventing or limiting the impact of threat actors performing lateral movement after successfully gaining initial access. When there is a need to perform remote administration, it should be performed securely through use of multi-factor authentication (MFA) and virtual private network (VPN).

Organisations can also consider restricting Internet access (e.g. via blacklisting or whitelisting), using a risk-based approach, especially where there is direct access from endpoints to large amounts of personal or sensitive data. When these endpoints, such as employee laptops, are compromised, there is a higher risk of personal data being exfiltrated.

Implement Routine Backups of Data

Organisations should implement routine backups to create and save copies of important files to external and offline storage devices. The backups should include immutable copies that will allow for system and data restoration in the event of a cybersecurity incident affecting data integrity. In addition, the backups 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. Organisations are advised to follow the 3-2-1 rule when performing backups:

- 3 copies of backups
- 2 different media formats of backups
- 1 set of backups stored off-site

Employ Web Application Firewalls (WAF)

Employing web application firewalls would allow organisations to filter malicious network traffic (e.g. SQLi) and "harden" their system configurations (e.g. for web server and firewalls). These WAF should have its signatures and rules updated regularly and enable any advanced SQL injection detection capabilities if present. The WAF should be used for monitoring any attempts at data exfiltration by monitoring outbound traffic for any suspicious traffic such as large payloads or communications with blacklisted IP addresses.

Develop Incident Response and Business Continuity Plans

Developing an incident response plan and conducting exercises to rigorously test the plan will allow organisations to respond swiftly and decisively in the event of a cyber attack. Organisations should also develop Business Continuity Plans (BCPs) with measures tailored to their needs to minimise the impact on business operations in the event of an attack.

Keep Essential Data Only

Organisations should only collect, process, store and retain data that are essential for business, operational or legal requirements. By only storing and retaining necessary data, the impact to an organisation due to a data breach can be minimised. Furthermore, additional resources required to protect these unnecessary data can be avoided by simply not collecting them in the first place. Some data minimisation practices include:

- Minimise collection of personal data
- Collect information on personal identifiers (e.g. national identification number) only when necessary
- Avoid continuous automatic collection of personal data
- Avoid repeatedly collecting the same data at different stages of an interaction

- Encrypt sensitive personal data that runs a higher risk of adversely affecting the individual
- Be aware of metadata (e.g. EXIF data in image files) embedded within files. Consider not collecting such data or removing them if not needed
- Be aware of caching information in temporary data stores and to regularly clear caches
- Ensure archival data past its retention period are diligently removed

Additional Resources:

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/dp-ict

MITRE ATT&CK Framework:

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