8th February 2024

Cyber Threat Alert: Surge in Attacks via Compromised Third-Party Service Providers

The Cyber Threat Intelligence Unit at BGD e-GOV CIRT has identified a surge in cyber-attacks targeting organizations through the compromise of third-party service providers. Recently, multiple organizations in Bangladesh have encountered data breaches. Some individuals employed by third-party service providers, tasked with offering technical support to various client organizations, have been targeted by information-stealing malware. Investigations revealed that the information-stealing malware covertly extracted sensitive data, including system information, browser cookies, and user account credentials, used to access client organizations.

Subsequently, threat actors utilized the stolen organizational credentials to gain unauthorized entry into the client organization's network. The attack rapidly escalated, employing sophisticated privilege escalation techniques, extensive discovery of critical assets, and lateral movement within the compromised organization.

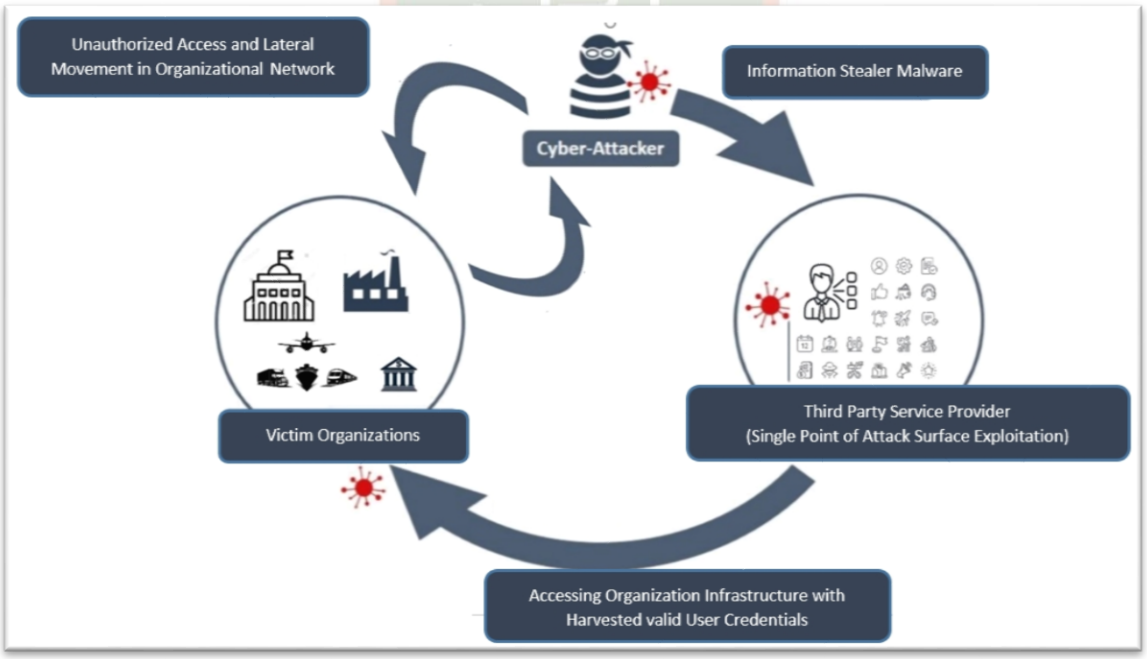

Fig: Infection Chain through Compromised Third-Party Service Providers

BGD e-GOV CIRT is publishing this alert to notify all organizations in Bangladesh about the substantial risks associated with compromises at third-party service providers. We urge organizations to take proactive measures to safeguard their assets from such potential attacks.

TLP:CLEAR

Phase	Description
Phase-1	Third-party service provider employee's machine infected with info-stealing malware.
Phase-2	- Info-stealer malware extracts sensitive information, including user account credentials.
	- Compromised credentials include access details used for providing support services to client organizations.
Phase-3	- Attackers utilize stolen organizational user credentials for unauthorized access.
	- Establishment and maintenance of footprints in the targeted organization lead to lateral movement.

Table: Primary Phases of Cyber Attacks through Compromised Third-Party Service Providers

Preventive measures for attack risks originating from third party service providers:

- **Access Control Policies:** Define clear access control policies specifying what resources, systems, and data the third-party employee is allowed to access. Use role-based access controls (RBAC) to assign permissions based on their specific job responsibilities.
- **Network Segmentation: I**solate third-party employees and grant them access only to the specific segments or VLANs required for their tasks. This limits their ability to move laterally within the network.
- **VPN and Remote Access Policies:** Implement a Virtual Private Network (VPN) for third-party employees requiring remote access. Enforce strict remote access policies, including multi-factor authentication (MFA) and secure VPN configurations.
- **User awareness programs:** Conduct regular phishing awareness training for employees. Educate users to exercise caution with email attachments/links.
- **Device Management:** Enforce policies for the devices used by third-party employees, including the requirement for up-to-date security software, endpoint protection, and compliance with the client organization's security standards.
- **Temporary Credentials:** Issue temporary credentials to third-party employees with a limited validity period. Regularly review and renew these credentials based on the duration of their engagement.
- **Monitoring and Auditing:** Implement monitoring and auditing mechanisms to track the activities of third-party employees on the client's network. This includes logging access attempts, changes to configurations, and any suspicious behavior.
- **Incident Response Plan:** Develop and communicate an incident response plan for third-party employees, outlining the steps to take in case of a security incident. Ensure they are aware of reporting procedures and collaborate with the client's incident response team.
- **Contractual Agreements:** Clearly define security requirements in contractual agreements with third-party vendors. Specify the security measures they must adhere to and the consequences for non-compliance.
- Report or inform BGD e-GOV CIRT regarding any cyber incident or suspicious activities within your infrastructure, through mail id: cirt@cirt.gov.bd.

A report has been already published at BGD e-GOV CIRT website on info stealer malware:
https://www.cirt.gov.bd/cyberthreatalert-infostealer

TLP:CLEAR