Subject **Advisory - Prevention Against Cyber Espionage (Advisory No 38) Jul 18**

1. **Introduction.** US CERT has published two alerts regarding attack by North Korean government referred to as "HIDDEN COBRA" targeted towards businesses sensitive and proprietary information. This targeted malicious attack has affected large number of countries.

2. **Summary of Malicious Application**

a. **Classification** . RAT/SMB attack

b. **Distribution.** Various phishing and drive-by attacks

c. **Malware Families**

(1) Joanap-Remote Access tool.

(2) Brambul-Server Message Block.

3. **Indicators of Compromise.** The malware makes following files on the infected system:-

a. **Registry Keys**

(1) HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security 125463f3-2a9c-bdf0-d890-5a98b08d8898.

(2) HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security f0012345-2a9c-bdf8-345d-345d67b542a1

b. Config file is encrypted written to a registry key: HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security.

4. **Malware Capabilities**

a. Hidden Cobra attack disrupts systems, files and regular operations.

b. Malware checks whether country is other than Korea and uptime of the system is at least 10 hours to operate.

d. **Joanap Capabilities**

(1) Malware exfiltrate data and drop further secondary payloads.

(2) Executable initializes proxy and peer-to-peer communication.

(3) Further, it manage to form botnets

e. **Bramble Capabilities**

(1) It's a Win32 brute force authentication worm providing shared 'access of files over network.

(2) Malware targets poorly secured networks and unsecured user accounts.

(3) Further sends system information back to Hidden Cobra actors via malicious email message.

(4) Malware have self-kill mechanism and control through command-line instructions.

5. **Recommendations.**

a. **Install and update well reputed antiviruses**. such as Kaspersky, Avira, Avast etc.

b. Maintain up-to-date patching and antivirus; enabling workstation firewalls; implementing 4nail and download - scanning to block suspicious 'attachments and files; restricting User permissions for software installations; and disabling Microsoft's File and Printer Sharing service, if not needed.

c. In case if indicators of compromise (para '3) are found in the system, pleasedisconnect the Computer from intemet and reinstall windows.

d. Update all software's including Windows OS, Microsoft Office and disable macros.

e. Don't download 'attachments from entrusted sources.