Date：2025/04/01

【Attack Alert】 Increasing Ransomware Attacks by Hacker Groups – Strengthen Preventive Measures

- Subject: 【Attack Alert】 Increasing Ransomware Attacks by Hacker Groups – Strengthen Preventive Measures
- Description:
  - Recently, multiple ransomware attacks have been reported targeting Taiwanese enterprises, schools, and hospitals. The hacker group **Crazy Hunter** exploits system vulnerabilities to conduct lateral attacks, then spreads ransomware across internal networks, encrypting files and causing service disruptions on multiple hosts.
  - The following known malicious programs have been identified: bb.exe, crazyhunter.exe, crazyhunter.sys, zam64.sys, go3.exe, and go.exe.
  - Since late January 2025, the Crazy Hunter ransomware group has targeted schools, hospitals, publicly listed companies, and corporate groups. We advise schools to verify whether their affiliated vendors have recently been affected by this ransomware group. If so, please exercise caution regarding business transactions with these vendors and assess potential data leaks. Schools are also requested to report any incidents to service@cert.tanet.edu.tw.
  - Preventive Measures:
    Prevention is key when dealing with ransomware attacks. In addition to strengthening data backups, organizations should establish offline backups, regularly assess server security, perform system security updates, and enhance password management.
    1. Regularly update passwords and increase password strength.
    2. Avoid using the same administrator password for multiple servers.
    3. Strengthen VPN security and remote access controls.
- Affected Platforms: All
- Recommended Actions:
  1. Regularly update system and antivirus software. If updates cannot be applied, deploy appropriate security measures.
  2. Be cautious with suspicious emails. Verify the sender’s authenticity and avoid opening unknown attachments. Scan email attachments before opening to detect and block malware. Watch for unusual filenames (e.g., exe.pdf, exe.doc, pdf.zip, lnk, rcs, exe, moc) that may indicate a malicious file.
  3. Implement network segmentation and isolation to reduce the number of vulnerable hosts.
  4. Enhance monitoring of privileged accounts, such as disabling accounts with excessive failed login attempts, logging login behaviors, and detecting suspicious activities.
  5. Adopt multi-factor authentication (MFA) to strengthen security.
  6. Regularly back up files** following the 3-2-1 backup rule:
     1. Keep at least three copies of your data.
     2. Use two different types of backup media.
     3. Store one backup copy offsite.
  7. Deploy Endpoint Detection and Response (EDR) solutions on critical systems to detect, investigate, and mitigate ransomware threats.
- Reference:

- https://www.twcert.org.tw/newepaper/cp-65-10042-adb7d-3.html

---

Network System Division
Computer and Communication Center9