JABATAN DIGITAL NEGARA, KEMENTERIAN DIGITAL

NOTA MAKLUMAN KETUA SEKTOR NCII KERAJAAN
JABATAN DIGITAL NEGARA
BIL. 3 TAHUN 2025

PADA 5 OGOS 2025

KETERANGAN	
No. Rujukan	NCII-NM-2025-0003
Tajuk Makluman	MAKLUMAN PENINGKATAN AKTIVITI ANCAMAN SIBER MENYASARKAN SISTEM KERAJAAN MALAYSIA YANG MENGGUNAKAN SUBDOMAIN .GOV.MY

PENGENALAN

Jabatan Digital Negara sebagai Ketua Sektor NCII Kerajaan ingin memaklumkan terdapat peningkatan aktiviti serangan siber yang menyasarkan sistem Kerajaan Malaysia, khususnya infrastruktur maklumat yang menggunakan subdomain gov.my. Serangan ini dipercayai didalangi oleh penyerang yang dikenali sebagai "BIGBROTHER"

Antara aktiviti serangan siber yang dikesan melibatkan kecurian identiti (credential leaks) dan akses tidak dibenarkan (unauthorised access) kepada akaun VPN dalaman, akses shell (contoh: SSH), pangkalan data rangkaian dan web serta perkongsian fail dalaman (file share). Serangan ini boleh dimanfaatkan oleh penyerang untuk menjalankan aktiviti pencerobohan, pencurian data atau pergerakan lateral (lateral movement) pada sistem dalaman agensi.

SISTEM YANG TERKESAN

Semua sistem, laman web, perkhidmatan dalam talian dan komponen rangkaian yang menggunakan subdomain .gov.my dianggap berisiko dan perlu diberi perhatian segera.

TINDAKAN PENGUKUHAN

Semua agensi hendaklah mengambil tindakan pengukuhan yang berikut:

PEMILIK SISTEM ICT

1. Melaksanakan aktiviti *threat hunting* berdasarkan penunjuk kompromi (Indicators of Compromise, IOC) yang terkini.

2. Melaksanakan semakan terhadap log bagi domain yang telah diceroboh dengan menyeluruh bagi memantau aktiviti yang tidak dibenarkan.

3. Memastikan tiada aktiviti *data exfiltration* dan *lateral movement* dalam sistem atau infrastruktur ICT.

4. Sekiranya pelayan disyaki atau telah dicerobohi, asingkan persekitaran pelayan, nyahaktifkan akaun dan tetapkan semula kata laluan serta mulakan tindakan pengendalian insiden.

5. **Bagi sistem atau infrastruktur maklumat yang tidak lagi aktif atau digunakan, pastikan akses kepada sistem ditamatkan dan sumber (resource) seperti *virtual machine* yang berkaitan tidak dihubungkan kepada rangkaian serta dibebaskan (release).**

6. Hentikan capaian yang mencurigakan atau tidak sah serta memantau trend capaian ke atas perkakasan, perisian, sistem ICT dan infrastuktur ICT.

7. Menyemak konfigurasi *firewall* dan menyekat atau mengehadkan akses ke port seperti port 3389 (RDP), 5900 (VNC) dan 22 (SSH) kecuali bagi port yang perlu diakses oleh umum.

8. Memasang tampalan (patch) dan kemas kini keselamatan (security updates) yang terkini serta halang skrip yang tidak sah dilaksanakan.

9. Memastikan perisian antivirus/*anti-malware* mempunyai *signature* yang terkini dan berfungsi.

10. Laksanakan tindakan pengukuhan bagi semua sistem yang boleh diakses melalui Internet.

11. Memastikan fungsi pengesahan identiti bagi mengakses ke sistem, pelayan dan rangkaian sentiasa diaktifkan dan melaksanakan pengesahan identiti pelbagai faktor (multifactor authentication) bagi mengurangkan risiko kecurian identiti.

12. Memastikan penggunaan kata laluan yang kukuh dan elakkan pendedahan.

13. Memastikan halaman login sebagai pentadbir sistem tidak boleh diakses melalui rangkaian luaran.

14. Membuat sandaran ke atas sistem dan data mengikut kekerapan yang telah ditetapkan.

15. Melaksanakan program kesedaran terhadap pengguna jabatan serta pihak yang terlibat dalam perkhidmatan berkaitan teknologi maklumat dan komunikasi berkaitan ancaman perisan kod hasad (malware) dan

menggalakkan penggunaan *End Point Protection* (EDR) untuk meningkat perlindungan terhadap perisan pencuri maklumat (infostealer) dan kod hasad (malware) serta sistem pencegahan kebocoran data (data leakage prevention).

16. Melaksanakan audit secara berkala ke atas akses dan konfigurasi sistem terutama infrastruktur yang dikategorikan sebagai NCII.

17. Sekiranya terdapat insiden yang berlaku dalam rangkaian dan persekitaran, laporkan kepada CSIRT agensi masing-masing dan Agensi Keselamatan Siber Negara di laman web https://www.nacsa.gov.my/incident_report_csirt.php.

18. Sekiranya insiden melibatkan infrastruktur maklumat kritikal negara, pelaporan kepada Agensi Keselamatan Siber Negara melalui sistem NC4 dan Ketua Sektor NCII Kerajaan Jabatan Digital Negara hendaklah dilaksanakan melalui e-mel ncii@jdn.gov.my.

19. Melaksanakan *compromise assessment* sekiranya berlaku insiden keselamatan siber.

PENGGUNA SISTEM ICT

1. Jangan klik sebarang pautan, lampiran, dokumen atau perisian yang mencurigakan.

2. Memastikan perisian/antivirus/*anti-malware* mempunyai *signature* yang terkini dan berfungsi.

3. Memastikan penggunaan kata laluan yang selamat dan tidak didedahkan.

4. Sekiranya terdapat insiden yang berlaku dalam rangkaian dan persekitaran, laporkan kepada CSIRT agensi masing-masing dan laksanakan imbasan keselamatan terhadap peranti yang digunakan untuk mengakses Sistem ICT.