UPDATE NOTIFIKASI INDIKASI AKTIFITAS GRUP APT MUSTANG PANDA PADA SISTEM DAN INFRASTRUKTUR PEMERINTAH INDONESIA

RINGKASAN EKSEKUTIF

1. Badan Siber dan Sandi Negara (BSSN) menerima laporan terkait adanya aktifitas Grup APT Mustang Panda yang diindikasikan melakukan penyusupan ke dalam jaringan menggunakan malware PlugX yang menargetkan Pemerintah Indonesia.
2. Dihimbau kepada pihak administrator sistem untuk segera menerapkan rekomendasi yang terdapat pada bagian akhir dokumen ini sebagai langkah tanggap insiden dan upaya pencegahan berupa deteksi dini aktivitas Grup APT Mustang pada sistem dan layanan pemerintahan Indonesia berbasis elektronik.

NOTIFIKASI INSIDEN

Terdapat Indicator of Compromise (IoC) dari aktifitas Grup APT Mustang Panda yang telah diberikan notifikasi sebelumnya berdasar Notifikasi Insiden dengan Nomor 266/IR/AT.01/09/2021 sebagai berikut :

1. Network Indicators
   - indoconka[.]com - PlugX C2 Domain
   - designcocos[.]com - PlugX C2 Domain
   - 167.179.94[.]196 - PlugX C2 IP
   - 158.247.208[.]159 - PlugX C2 IP
   - 149.28.156[.]153 - Cobalt Strike C2 IP
2. Historical PlugX C2s Hosting indoconka[.]com and designcocos[.]com :
   - 185.239.226[.]21
   - 45.19.171[.]9
   - 185.239.226[.]38
   - 103.56.55[.]67
   - 95.179.171[.]84
   - 36.69.235[.]174
   - 45.76.185[.]72

Dari IoC tersebut, terdapat penambahan IoC yang kami dapatkan sebagai berikut :

- 103.56.55[.]11
- 141.164.41[.]93
- 149.248.20[.]183
- 149.28.156[.]43
- 80.240.24[.]215
- microsymantec[.]com

Direktorat Operasi Keamanan Siber BSSN menghimbau agar segera melakukan langkah tanggap insiden dan upaya mitigasi lebih lanjut yang direkomendasikan untuk pihak administrator sistem dan layanan:

1. Menambahkan IoC tersebut pada perimeter keamanan yang dimiliki serta melakukan pemantauan terhadap aktifitas yang terdeteksi berkomunikasi dengan IoC tersebut.
2. Melakukan pengecekan di perangkat perimeter keamanan yang dimiliki apakah terdapat koneksi dari internal organisasi yang terhubung dengan IoC tersebut.
3. Melakukan *containtment* terhadap perangkat komputer dan analisis lebih lanjut terhadap perangkat yang terhubung ke IoC tersebut.

Jakarta, 16 September 2021