

10 ANCAMAN UTAMA

Trojan dan Mass Mailer terus mengganggu pengguna

Fortinet, peneraju dan penyedia penyelesaian pengurusan ancaman bersatu, baru-baru ini mengumumkan 10 ancaman utama paling berisiko yang dilaporkan pada bulan Jun lalu. Laporan itu diperolehi daripada sistem sekuriti multi-ancaman FortiGate seluruh dunia, dijalankan oleh sekumpulan penyelidik Sekuriti Global Fortinet.

Menerusi laporan tersebut, Trojan W32/Dialer.PZ!tr mendahului carta dengan 13.43% virus dikesan tersebar meluas di seluruh dunia. Ini diikuti dengan W32/Bagle.DY@mm iaitu ancaman emel gadang dengan 10.05% dikesan. Seterusnya dengan peratusan 7.11% dikesan adalah W32/Netsky.P@mm dan ancaman exploit HTML/Iframe_CID!exploit dikesan sebanyak 5.90%.

Ancaman-ancaman lain yang dikesan sepanjang bulan Jun lalu ialah W32/ANI07.A!exploit (3.52%), W32/Grew.A!worm (3.50%), W32/Bagle.GT@mm (2.43%), W32/Sober.AA@mm (1.98%), W32/Stration.JQ@mm (1.89%) dan W32/Salicy.Q (1.75%).

Secara keseluruhan 10 ancaman ini adalah konsisten berikutan Grew.A, Bagle GT, Sober AA, Stration JQ dan ANI07 masih kekal di posisi yang sama seperti sebelumnya. Salisty.Q memasuki carta ancaman paling banyak dilaporkan, sekali gus menolak serangan phishing BankFraud.E dari senarai. ANI07 pula merupakan ancaman berasaskan Web dan dikatakan lebih banyak pada bulan Jun lalu berikutan kehadirannya sudah lama dipasang dan menunggu untuk disebarkan oleh individu tidak bertanggungjawab.

Ancaman paling menarik perhatian kali ini adalah Dialer.PZ yang sekali lagi mendahului carta. Bulan Mei lalu, Fortinet mengumumkan kitaran hidup W32/Dialer.PZ!tr disebarkan oleh rekan dinamik dan terperinci daripada barisan pemasangan, laporan statistik pintar, strategi pelaksanaan dan muatan bayar (payload). Ia paling banyak ditemui di Mexico dan Amerika Syarikat serta beberapa bahagian lain seluruh dunia.

"Musim ini pencipta Malware lebih terdorong oleh prospek serangan bermusim dan Malware yang dipakejkan bersama. Pencipta menempatkan malware dalam satu pakej dengan harapan ianya tidak dapat dikesan dan cuba mencerooboh sempadan virtual," kata Derek Manky, Jurutera Penyelidikan Sekuriti Fortinet.

Manky turut memberitahu bahawa pencipta Malware dan ancaman-ancaman ini telah mengubah komponen dalam proses penciptaan dengan membungkus W32/Dialer.PZ!tr variasi terkini pada bungkusan masa-jalan popular UPX. Sampel pertama malware yang menggunakan cara ini dikesan pada 21 Jun lalu.