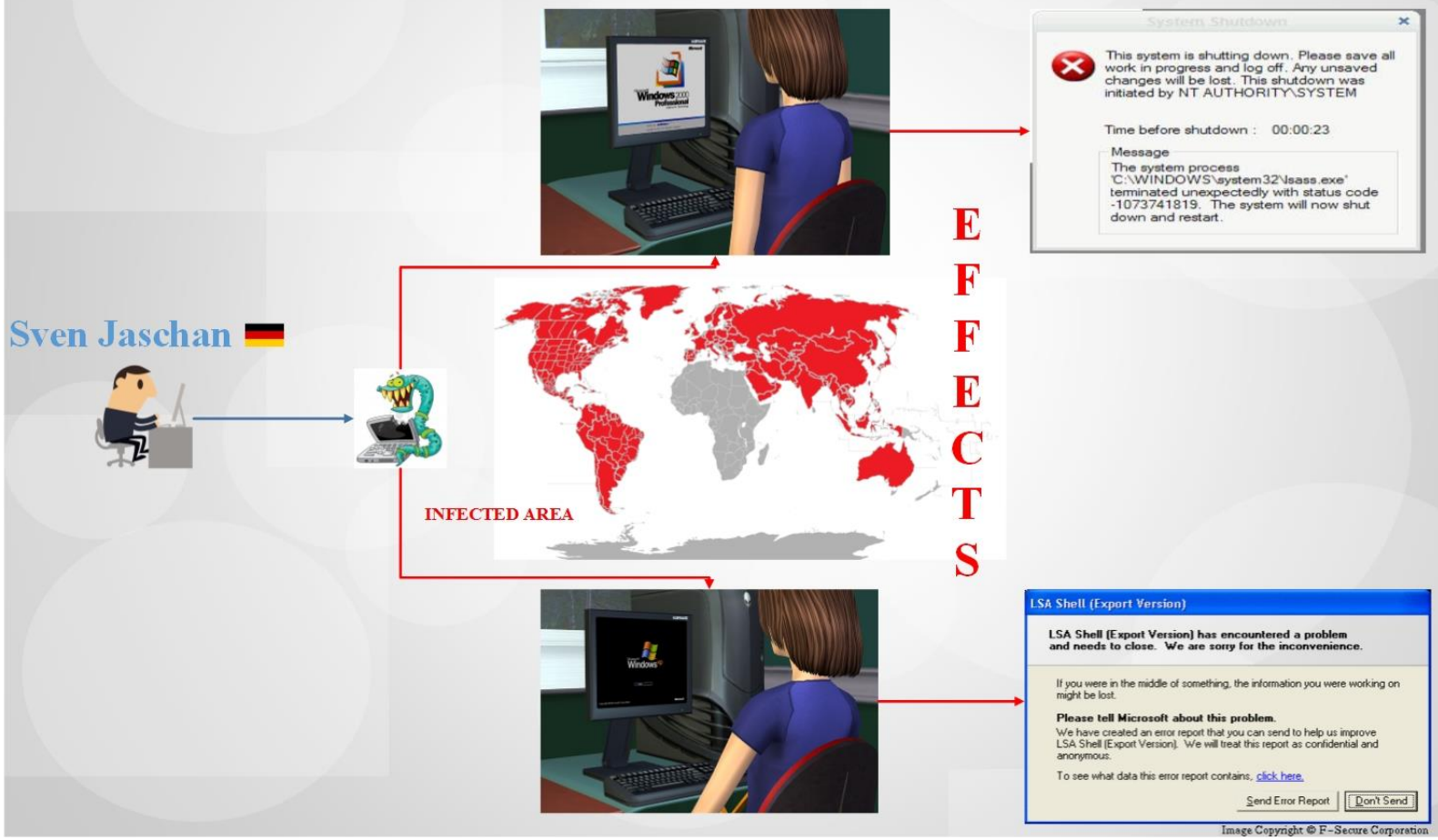
Sasser Worm
2004



Sasser Worm

Sasser worm adalah sebuah *worm* yang menyerang sistem operasi Windows 2000 dan Windows XP pada tahun 2004, dimana komputer yang terinfeksi *worm* ini akan menjadi lambat atau *crash* sehingga akan terus menerus melakukan *reboot*. Sasser Worm dibuat oleh mahasiswa ilmu komputer di Jerman bernama Sven Jaschan. Penyerang menjalankan FTP *Server* pada *port* 5554 dan mencoba menghubungkan ke IP acak pada *port* 445. Ketika terhubung maka *worm* mengirim *shellcode* pada komputer yang terhubung untuk menjalankan *remote shell* pada *port* TCP 9996. *Worm* akan menggunakan *shellcode* untuk mengkoneksikan kembali ke FTP *Server* penyerang pada *port* 5554 dan menyalin *worm* tersebut. Sven Jaschan berhasil ditangkap pada tahun 2005 dan tidak dipenjara karena Sven berumur 18 tahun awal. Sven hanya dikenai sanksi untuk melayani masyarakat selama 21 bulan.

Efek Sasser Worm pada Dunia

Benua Eropa

Sampo bank (sekarang menjadi Danske bank) menutup semua 130 cabang selama beberapa jam setelah perusahaan tersebut terinfeksi *worm* Sasser. Tidak ada kerugian atau kebocoran data selama terinfeksi Sasser Worm.

Penerbangan di British airways delay karena Sasser worm menginfeksi pada terminal keempat yang belokasi di London Heathrow Airport dan menginfeksi call centers di Manchester dan Glasgow.

Menginfeksi komputer yang ada di gedung pengadilan nasional Spanyol sehingga memblokir hakim yang akan menggunakan komputer tersebut.

Benua Asia

Transaksi perbankan dan layanan post di negara Taiwan menjadi terganggu karena 1600 komputer telah terinfeksi Sasser worm.

Dua departemen pemerintah dan beberapa rumah sakit di Hong Kong terinfeksi Sasser Worm.

Asan Medical Center, rumah sakit di Korea mengalami perhambatan dalam merawat pasien karena harus mencari dan menulis *record* pasien dengan pena dan kertas.

Perusahaan Lotte Group ditutup sehari karena Sasser Worm

Benua Amerika

Delta airlines menunda dan membatalkan sejumlah penerbangan karena komputer mereka terinfeksi Sasser worm

6.000 dari 17.000 komputer di Universitas Texas terinfeksi Sasser Worm.

Perusahaan Goldman Sachs terinfeksi Sasser Worm.

Benua Australia

RailCorp di Australia terinfeksi Sasser Worm sehingga 300.000 penumpang terdampar karena *worm* mematikan jaringan radio, beberapa stasiun ditutup dan hanya 20 kereta yang berfungsi dalam jangka waktu tertentu.

Bank Westpac harus menggunakan pena dan kertas untuk melayani konsumen karena terinfeksi Sasser Worm.

Pencegahan Sasser Worm

- Update Windows
- Aktifkan Firewall
- Gunakan Anti-virus.