Nama : Ratna Dewi A

NIM : 1310651068

Kelas : D

1.

Informasi Tata Kelola Keamanan dan Manajemen Risiko

- ✓ **Aktiva**

Aset adalah sumber daya berharga yang kita lindungi. Aset dapat berupa data, sistem,orang, bangunan, properti, dan sebagainya. Nilai dari aset akan menentukan bagaimana pengamanannya.

- ✓ **Ancaman dan kerentanan**

Ancaman adalah segala sesuatu yang berpotensi menyebabkan kerusakan pada aset. Untuk memiliki risiko, ancaman harus terhubung ke kerentanan. Hubungan ini dinyatakan oleh rumus: **Resiko ¼ threatvulnerability**

- ✓ **Matrix Analisis Resiko**

Matrix Analisis Resiko menggunakan kuadran untuk menentukan kemungkinan dampak resiko yang akan dimiliki.Tujuan dari matriks adalah untuk mengidentifikasi resiko kemungkinan / high-konsekuensidan meminimalisirnya / lowconsequence risiko

- ✓ **Nilai Aktiva**

Nilai Aktiva (AV) adalah nilai aset yang kita lindungi. Aset berwujud (seperti komputer atau bangunan) yang mudah dihitung. Menurut Deloitte, ada tiga metode untuk menghitung nilai aset tidak berwujud, pendekatan pasar, pendekatan pendapatan, dan pendekatan biaya:

- Pendekatan Pasar: Pendekatan ini mengasumsikan bahwa nilai wajar aset mencerminkanharga yang sebanding aset telah dibeli dalam transaksi di bawah kondisi yang sama.

- Pendekatan Pendapatan: Pendekatan ini didasarkan pada premis bahwa nilai dari keamanan atau aset adalah nilai sekarang dari kapasitas produktif di masa mendatang.
- Pendekatan Biaya: Pendekatan ini memperkirakan nilai aset dengan mengacu biaya yang akan dikeluarkan untuk membuat atau mengganti aset.

✓ **Analisis Risiko Kualitatif dan Kuantitatif**

Merupakan dua metode untuk menganalisis risiko. Analisis Risiko Kuantitatif menggunakan metrik keras, seperti dolar. Risiko Kualitatif Analisis menggunakan nilai perkiraan sederhana. Kuantitatif lebih objektif; kualitatif lebih subjektif. Analisis Risiko Hybrid menggabungkan dua: menggunakan kuantitatif analisis untuk risiko yang mungkin mudah dinyatakan dalam seperti uang.

✓ **9-langkah panduan proses Analisis Resiko:**

a) Sistem Karakterisasi
b) Ancaman Identifikasi
c) Kerentanan Identifikasi Analisis
d) Kontrol Penentuan
e) Kemungkinan
f) Analisa Dampak
g) Penentuan Analisis Resiko
h) Kontrol Rekomendasi
i) Hasil Dokumentasi

✓ KEAMANAN INFORMASI DATA

Keamanan Informasi Pemerintahan adalah keamanan informasi di tingkat organisasi: manajemen senior, kebijakan, proses, dan staf. Itu juga merupakan prioritas organisasi disediakan oleh kepemimpinan senior, yang diperlukan untuk informasi yang berhasil program keamanan. Kebijakan keamanan dan dokumen terkait Dokumen seperti kebijakan dan prosedur adalah bagian yang diperlukan dari setiap sukses program keamanan informasi.

- ✓ **Prosedur**

  Prosedur adalah panduan langkah-demi-langkah untuk menyelesaikan tugas. Berikut ini adalah contoh prosedur sederhana untuk membuat user baru:

  1. Menerima formulir permintaan baru-pengguna dan memverifikasi kelengkapan.
  2. Pastikan bahwa manajer pengguna telah menandatangani formulir.
  3. Pastikan bahwa pengguna telah membaca dan setuju dengan kebijakan keamanan akun pengguna.
  4. Klasifikasikan peran pengguna dengan mengikuti prosedur peran-tugas NX-103.
  5. Pastikan bahwa pengguna telah memilih "kata rahasia," seperti gadis ibu merekanama, dan masukkan ke dalam profil akun help desk.
  6. Buat account dan menetapkan peran yang tepat.
  7. Menetapkan kata rahasia sebagai password awal dan mengatur "Angkatan pengguna untuk mengubah password pada login berikutnya untuk 'Benar'. "
  8. E-surat dokumen Akun Baru ke pengguna dan manajer mereka.

Pemilik data (juga disebut pemilik informasi atau pemilik bisnis) adalah manajemenkaryawan yang bertanggung jawab untuk memastikan bahwa data yang spesifik dilindungi. Pemilik Data menentukan Data label sensitivitas dan frekuensi backup data. Sebuah perusahaan dengan beberapa lini bisnis mungkin memiliki beberapa pemilik data.

FAKTA CEPAT

ISO 17799 memiliki 11 daerah , dengan fokus pada kontrol keamanan informasi spesifik :

1) Kebijakan
2) Organisasi keamanan informasi
3) Manajemen 3. Aset
4) Keamanan 4. Sumber daya manusia
5) Keamanan fisik dan lingkunganKomunikasi dan manajemen operasi Kontrol 7.
6) Access

7) Sistem informasi akuisisi , pengembangan , dan pemeliharaan
8) Informasi manajemen insiden keamanan
9) Manajemen kontinuitas 10. Bisnis
10) Compliance2

- ✓ **ITIL**

ITIL (Information Technology Infrastructure Library) adalah suatu kerangka kerja untuk menyediakan pelayanan terbaik di IT Service Management (ITSM) . Informasi lebih lanjut tentang ITIL tersedia di http://www.itil-officialsite.com .
ITIL berisi lima " Service Management Praktek -Core Bimbingan " publikasi :
• Strategi Layanan
• Desain Layanan 58 BAB 3 Keamanan Informasi Pemerintahan
• Layanan Transisi
• Operasi Layanan
• Peningkatan Pelayanan terus menerus

- ✓ **Sertifikasi dan Akreditasi**

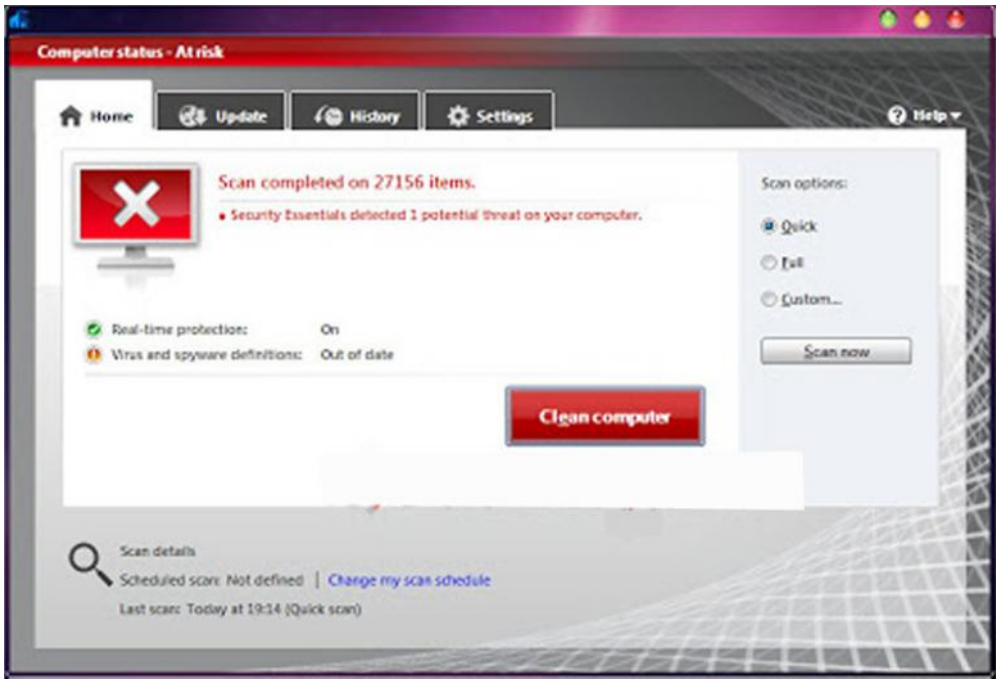
Sertifikasi adalah pemeriksaan rinci yang memverifikasi apakah sistem memenuhi persyaratan keamanan . Akreditasi adalah penerimaan dataowner tentang risiko yang diwakili oleh sistem itu. Proses ini disebut Sertifikasi dan Akreditasi atau C & A .

- ✓ **IKHTISAR TUJUAN UJIAN**

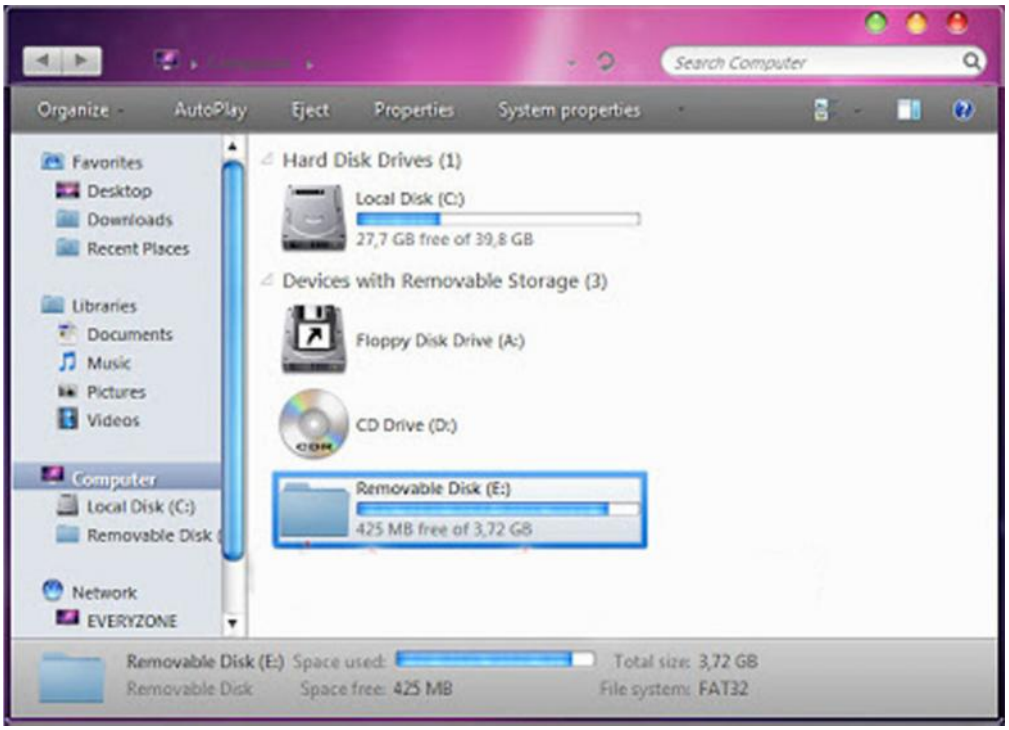
Pemerintahan keamanan informasi menjamin bahwa organisasi memiliki informasi struktur , kepemimpinan , dan bimbingan yang benar . Tata Kelola membantu memastikan bahwa perusahaan memiliki kontrol administrasi yang tepat untuk mengurangi risiko . Analisis Risiko (RA) membantu memastikan bahwa organisasi benar mengidentifikasi , menganalisis , dan meringankan risiko .

2.

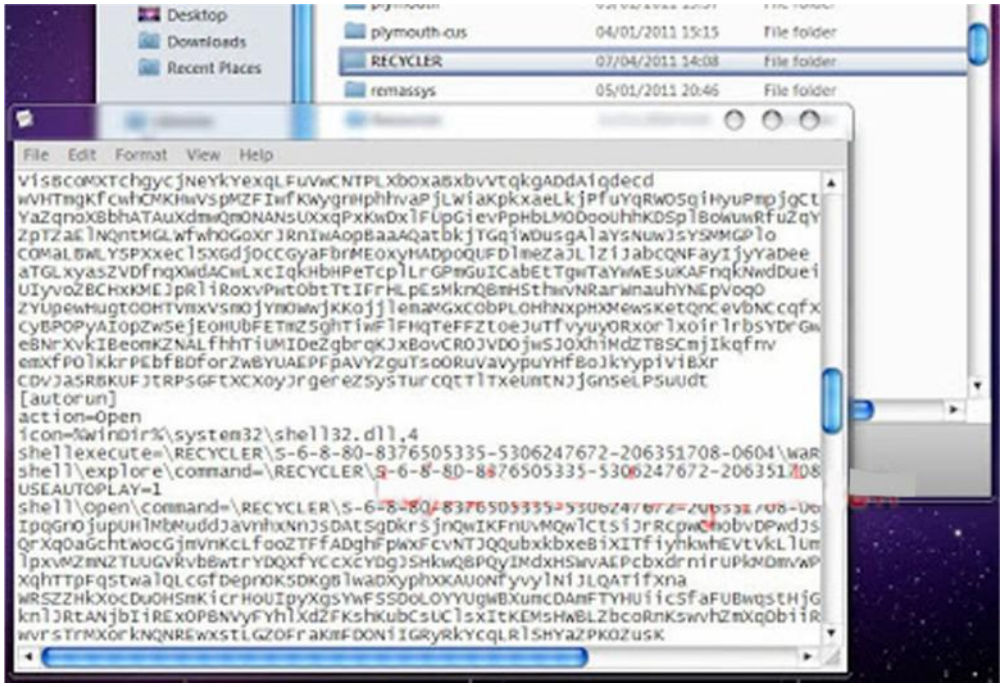
Membersihkan Virus Ramnit Dengan Miscrosoft Security Essentials (MSE)



Miscrosoft Security Essentials (MSE) adalah anti virus resmi yang dikeluarkan Microsoft untuk menanggulangi penyebaran malware. Mengambil contoh tiga virus yang menurut kebanyakan orang paling banyak menyebabkan masalah adalah virus Sality, Virut dan Ramnit. Dua virus pertama adalah virus lama, namun karena banyaknya varian dari keduanya, menjadikan virus tersebut sulit dimusnahkan. Virus yang akhir-akhir ini banyak diresahkan adalah Ramnit variant. Ramnit menyebar dengan cepat dan varian virus ini cukup banyak. Ramnit tergolong malware berbahaya dan sulit dibersihkan. Sekali saja sebuah sistem terinfeksi olehnya, maka pembersihan sistem tidak dapat dilakukan dengan sebarang anti virus.

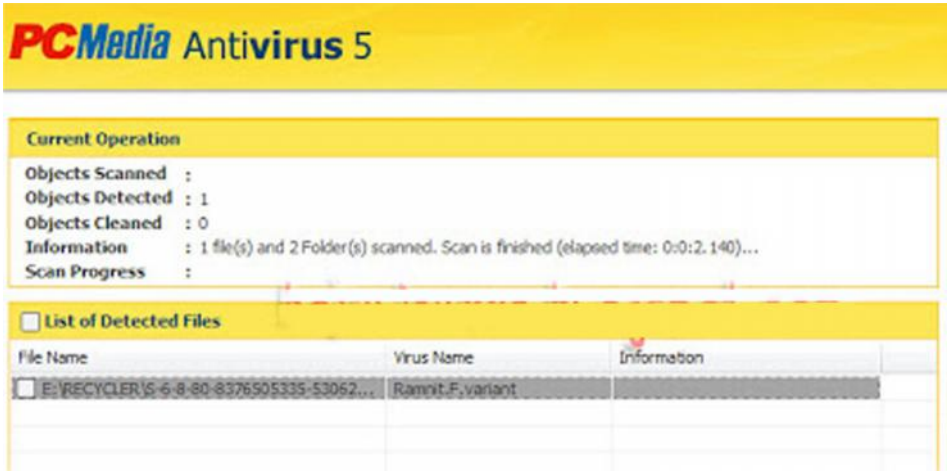


Ikon berubah menjadi folder pada Flashdisk yang terinfeksi Ramnit

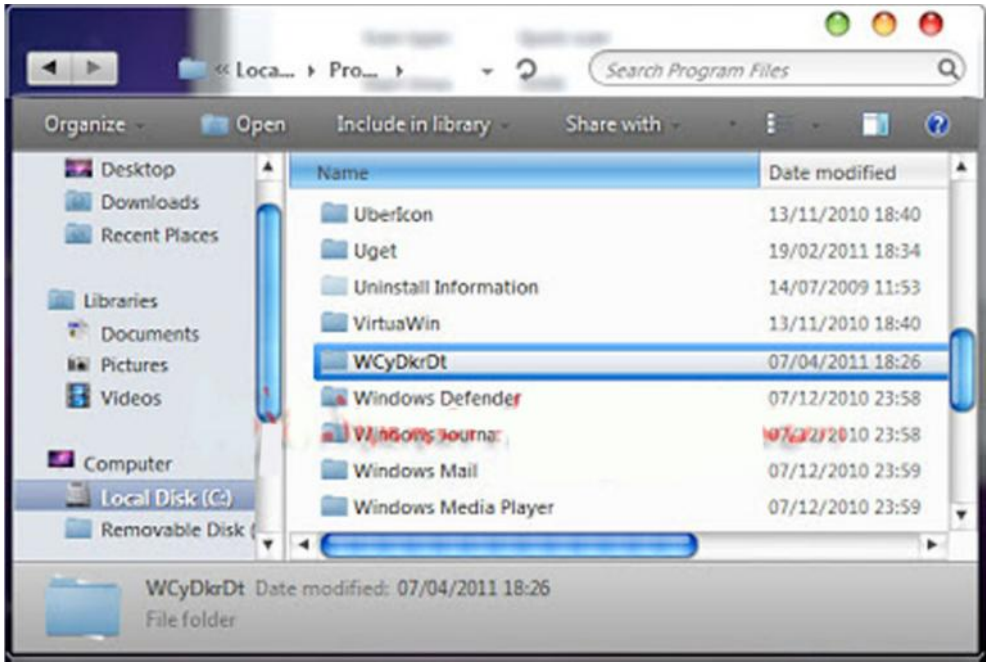


Ramnit menciptakan file autorun.inf, Copy of Shortcut to (1).lnk sampai 4 dan folder RECYCLER berisi file virus pada flashdisk.

✓ **Membersihkan Virus Ramnit dengan MSE**

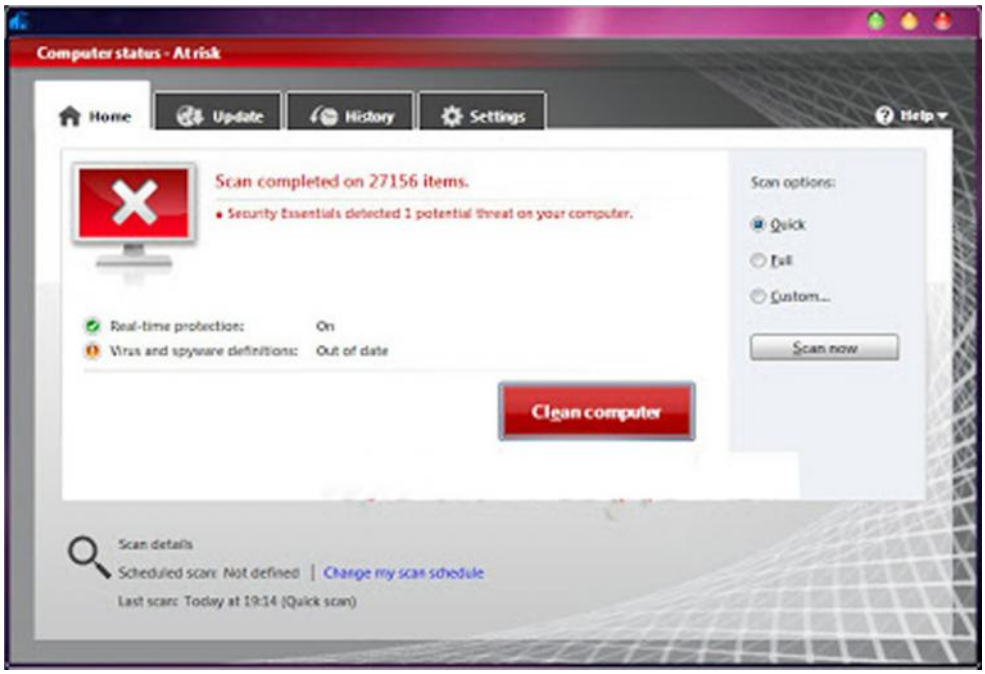


Untuk membersihkan virus ramnit cukup menggunakan **Miscrosoft Security Essentials (MSE)** yang terupdate. Contoh : membersihkan komputer dari Trojan:win32/Ramnit.A menurut **MSE** dan Ramnit.F.variant menurut **PCMAV 5.0**.

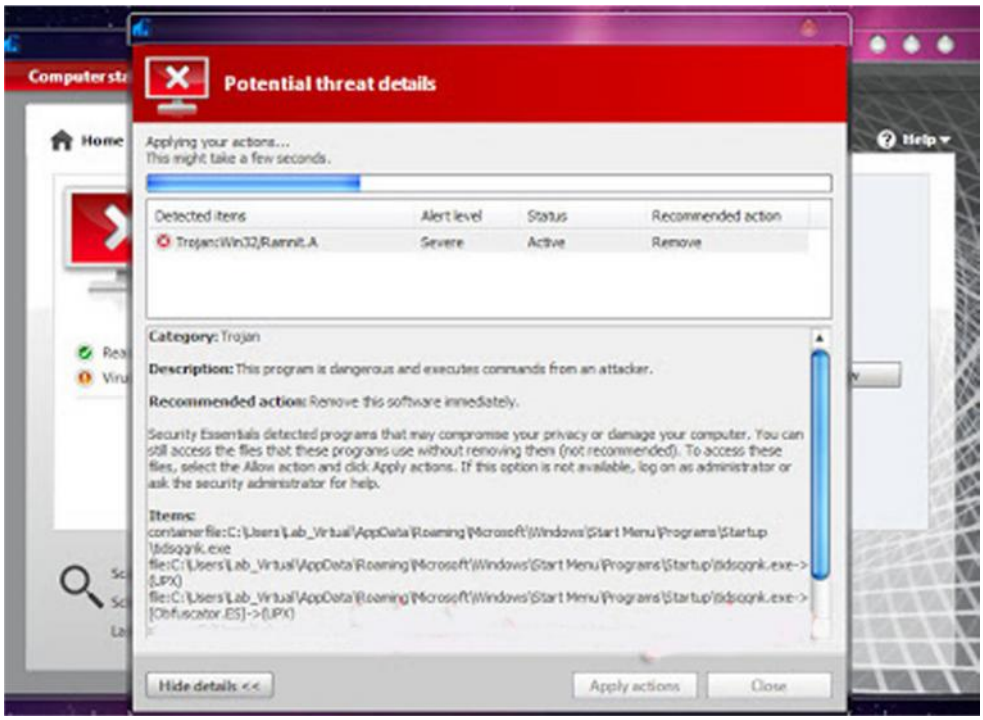


Ramnit menyerang sistem akan membuat folder acak berisi induk virus yang akan dijalankan otomatis saat komputer dijalankan. Folder virus tersebut diletakkan pada folder Program Files. Selain itu, Ramnit juga meletakkan file virus pada folder Startup dan memanipulasi userinit pada registry. Variant lain mungkin memiliki cara dan file virus yang berbeda dengan contoh diatas.

Untuk membersihkan virus Ramnit variant ini, silahkan download dan instal MSE terbaru. Saat mendownload MSE sebaiknya Anda juga mendownload virus definisi MSE terbaru untuk diinstal secara manual setelah proses instalasi MSE selesai, karena kemungkinan Ramnit akan menghalangi Anda untuk mengupdate virus definisi secara online. Bagi pengguna Windows XP SP3, disamping membutuhkan kedua file MSE tersebut juga memerlukan file update Windows Installer versi 3 (KB942288) atau yang lebih baru dan instalasi beberapa patch akan diminta saat menginstal MSE pada Windows Xp yang tidak pernah diupdate.

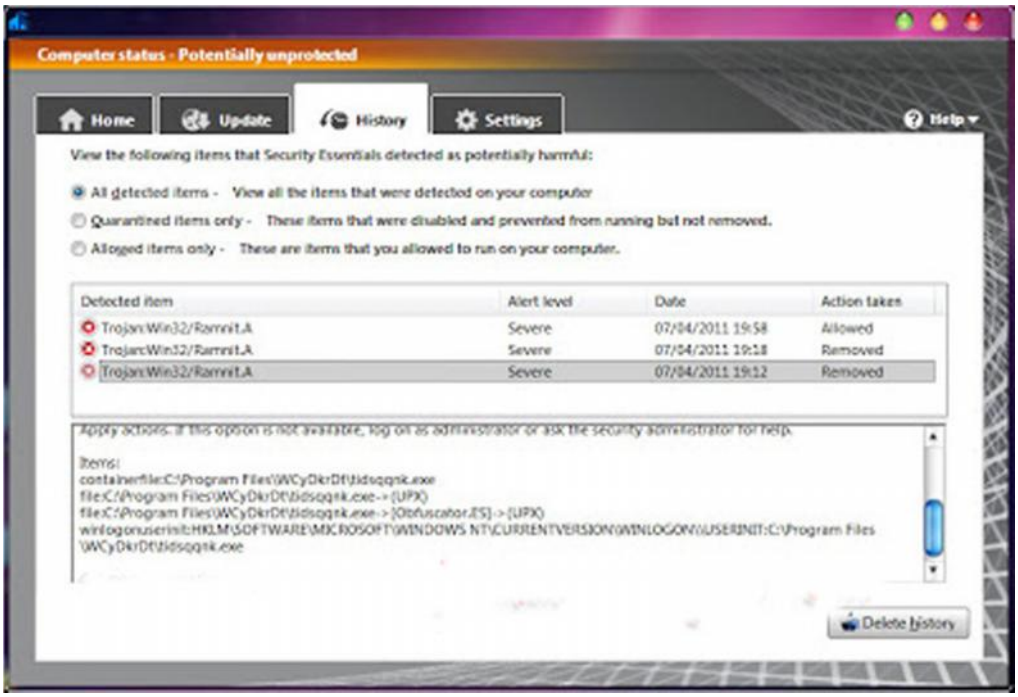


MSE menemukan Rumnit yang aktif di memori



Pembersihan memori dari infeksi Ramnit

Setelah memori berhasil dibersihkan dari Ramnit, restart komputer lalu scan semua isi hardisk dan flashdisk yang Anda gunakan dengan **MSE**.



Scan total menggunakan MSE untuk membersihkan komputer dari infeksi Ramnit