Teleko

Yakni berfokus pada kerahasiaan, integritas, dan ketersediaan data di
gerak.
satu domain terbesar di Tubuh Umum
Domain ini juga salah satu domain yang paling teknis yang mendalam, yang membutuhkan pengetahuan teknis
turun
untuk
paket,segmenframe Dan header mereka

komunikasi
Pengirim atau menerima pada satu waktu saja (tidak bersamaan), seperti
walkie-talkie.
Full-duplex
komunikasi mengirim dan menerima secara bersamaan, seperti
dua orang memiliki percakapan tatap muka.

Komunikasi keamanan
Melindungi data dalam gerak adalah salah satu tantangan yang paling kompleks yang kita hadapi. Antar
net menyediakan murah global yang komunikasi-dengan sedikit atau tanpa built-in kerahasiaan.
keamanan mengasumsikan bahwa jaringan eavesdropper bisa mengendus semua paket yang dikirim
antara client server dan otentikas seperti:
PAP (Password Authentication Protocol) mengirimkan username dan password dalam teks-jelas.
CHAP (Tantangan-Handshake Authentication Protocol)
melakukan otentikasi yang lebih aman.Dan bergantung pada rahasia bersama: password. Sandi
aman diciptakan (seperti selama akun pendaftaran) dan disimpan di server CHAP.
Karena kedua pengguna dan berbagi server yang CHAP rahasia (password plaintext),dapat menggunakan rahasia
yang aman untuk otentikasi.
802.1X.
EAP dirancang untuk menyediakan otentikasi pada Layer
2 (itu adalah "port berdasarkan," seperti port pada switch), sebelum simpul menerima alamat IP. Ini
tersedia untuk kedua kabel dan nirkabel, tetapi paling sering digunakan pada WLAN.
Klien EAP disebut pemohon a, yang meminta otentikasi ke server yang disebut
authenticator
VPN
Virtual Private Networks (VPN) data yang aman dikirim melalui jaringan tidak aman.
seperti T1, virtual_transport
tually. Mur dan baut dari VPN melibatkan otentikasi aman, kriptografi
hash seperti SHA-1 .
PPP
PPP (Point-to-Point Protocol) adalah Layer 2 protokol yang menambahkan kerahasiaan, integritas yang
ritas, dan otentikasi melalui point-to-point.

Ipsec
memberikan keamanan. Untuk mengatasi kurangnya keamanan di Layer 3, IPsec (Internet Protocol

SSL dan TLS
Secure Sockets Layer (SSL) dirancang untuk melindungi HTTP Data: HTTPS menggunakan port TCP 443. TLS (Transport Layer Security).TLS 1.2digunakan untuk mengenkripsi berbagai jenis
data dan dapat digunakan untuk terowongan protokol IP lainnya untuk membentuk koneksi VPN.

VoIP
Voice over Internet Protocol membawa suara melalui jaringan data keuntungan dari paket-switched jaringan, seperti biaya yang lebih rendah dan ketahanan, dengan
telepon dsb.

(WLAN) Wireless Local Area Networks
Mengirimkan informasi melalui elektromagnetik gelombang (seperti radio) atau cahaya Persepsi ini biasanya salah tempat. Bentuk yang paling umum
jaringan data nirkabel 802.11 standar nirkabel, dan yang pertama 802.11-standar
dard dengan keamanan yang wajar 802.11i.

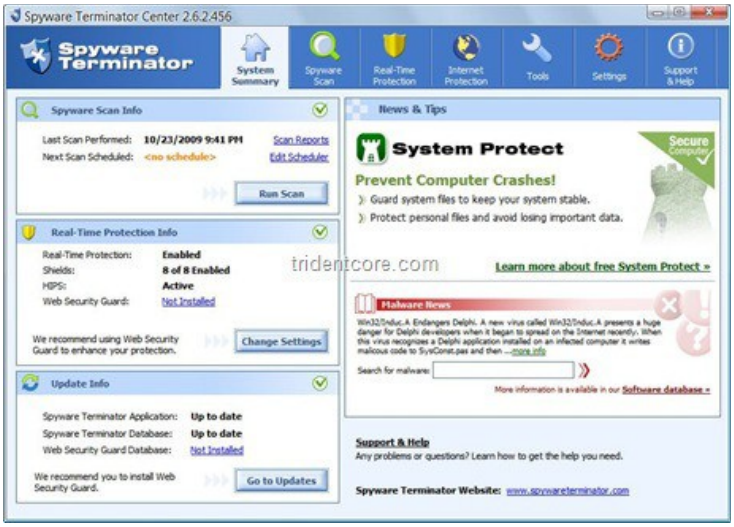
FHSS, DSSS, dan OFDM
Frekuensi-Hopping Spread Spectrum (FHSS) dan langsung Urutan Menyebar alamiah lainnya
trum (DSSS) adalah dua metode untuk mengirimkan lalu lintas melalui sebuah band radio. Beberapa band, seperti 2,4 GHz ISM band, bisa cukup tercemar dengan gangguan: Bluetooth, beberapa
telepon nirkabel, beberapa 802.11 nirkabel, monitor bayi, dan bahkan oven microwave dapat
menyiarkan atau mengganggu band ini.

RFID
Radio-Frequency Identification (RFID) adalah teknologi yang digunakan untuk membuat kabel
RFID tag pasif tidak memiliki baterai dan juga bergantung pada RFID pembaca
sinyal untuk daya.

Remote akses
crit- sebuah
control ical. Ini termasuk menghubungkan pengguna ponsel melalui Cable Modeminstant messaging dan teknologi rapat jarak jauh.

Akses konsol Remote desktop
Banyak pengguna memerlukan akses remote untuk konsol komputer '. Tentu, beberapa bentuk
saluran aman seperti IPSec VPN, SSH, atau tunnel SSL harus digunakan untuk memastikan con
fidentiality koneksi, terutama jika koneksi berasal dari luar
organisasi.

Spyware Terminator



Spyware Terminator merupakan antispyware yang mengintegrasikan fitur penuh tanpa terkecuali dan fleksibilitas yang luar biasa. Spyware Terminator menawarkan fitur antispyware gratis, update otomatis gratis, scan terjadwal gratis, antivirus terintegrasi gratis (optional), dukungan gratis dan gratis untuk penggunaan pribadi dan komersial. Kurang apa lagi? Oh ya ada satu lagi sebenarnya, fitur offline update. Jadi dapat mengupdate database spyware tanpa harus terkoneksi ke internet.

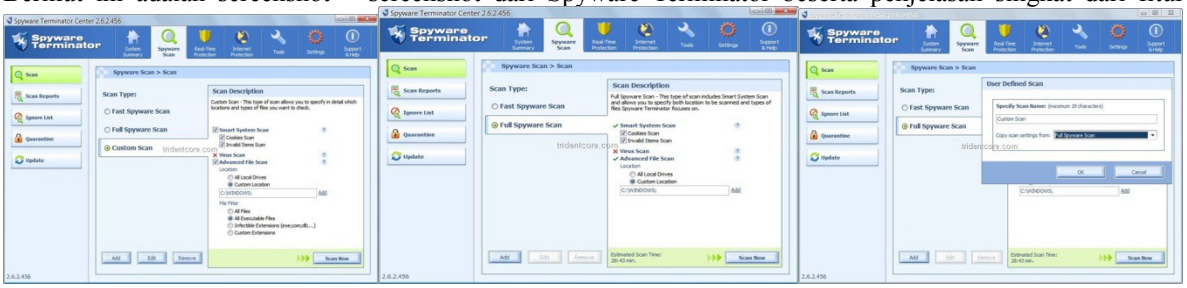
Versi terbaru dari program antispyware terpopuler, Spyware Terminator versi 2.5. Program keamanan anti spyware yang berlisensi gratis ini dikenal dengan fitur deteksi spyware dan HIPS yang sangant spektakuler. Full Featured Antispyware. Semua fitur-fitur di versi terbaru ini telah ditingkatkan, yang paling mencolok adalah tampilan GUI, tata letak yang lebih rapi dan lebih jelas.

Sejak versi 2.5 ke atas, Spyware Terminator telah mengurangi beban resourcenya dan lebih ringan daripada sebelumnya. Fitur HIPS yang telah disempurnakan dan telah ditingkatkan dengan menyertakan penjelasan langsung terhadap proses yang bersangkutan beserta informasi detail dari proses tersebut.

Fitur HIPS telah diperbaharui dengan menggunakan metode “Whitelist” dan “Blacklist”, ditambah lagi sebuah metode berdasarkan “child process” dan ‘all modules”. Jadi semua proses dari proses awal (master proses) akan dianggap whitelist (untuk metode “child process”) sementara metode “all modules” akan memberi hak akses terhadap modul-modul proses (dll, xml, bin, dan lain-lain) dibawah master proses.

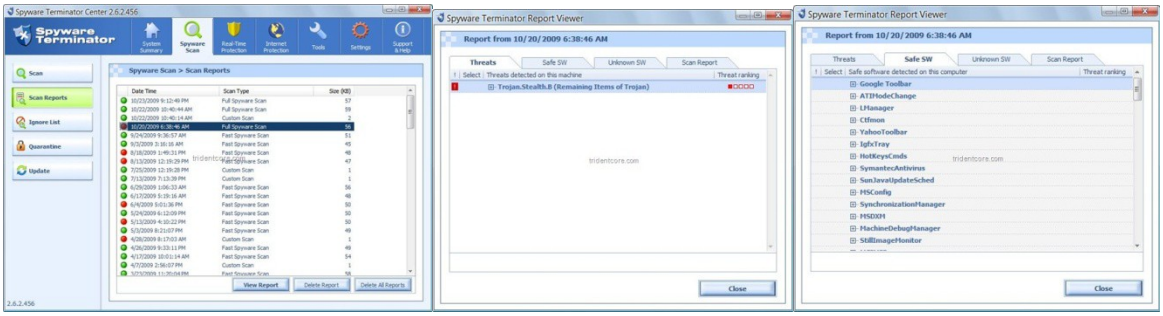
Fitur update pun mirip dengan Norton AntiVirus 2010 dengan menggunakan metode “yang seperlunya”, jadi proses update hanya mendownload file-file update yang diperlukan, alhasil beban koneksi internet jadi ringan.

Berikut ini adalah screenshot – screenshot dari Spyware Terminator beserta penjelasan singkat dari fitur yang



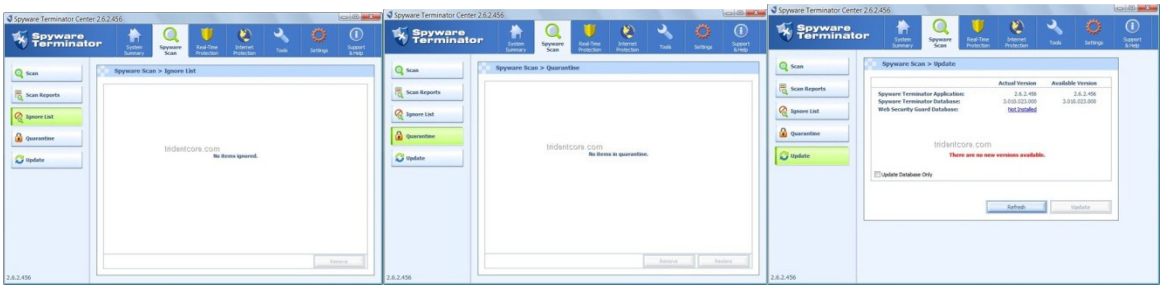
Pada tab Spyware Scan, disediakan 2 pilihan awal untuk memulai pemeriksaan sistem terhadap spyware. Fast Spyware Scan dan Full Spyware Scan, untuk Fast Spyware scan ditujukan untuk memeriksa direktori atau lokasi yang kerap menjadi sasaran spyware sedangkan Full Spyware Scan akan memeriksa seluruh file di dalam partisi sistem operasi.

Pengguna bisa menambahkan sebuah profil baru dalam tab Spyware Scan, dengan klik tombol “Add” dibawah lalu beri nama pada profilnya, lalu pilih metode scan-nya apakah Fast atau Full lalu setelahnya bisa dikonfigurasi lebih lanjut untuk direktori yang akan diperiksa (scan).



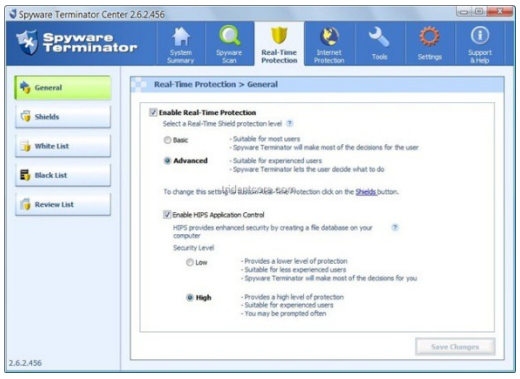
Masih dalam tab Spyware Scan namun sekarang beralih ke sub-tab Scan Result, disini pengguna dapat melihat semua laporan pemeriksaan sistem terhadap spyware yang telah dilakukan oleh Spyware Terminator. Pilih salah satu laporan dan klik tombol “View Report”, pada tampilan Spyware Terminator Report Viewer dapat dilihat berbagai informasi terkait dengan hasil scan tertentu.

Terdapat 4 tab dengan masing – masing informasi yang berbeda, dari tab paling kiri ditampilkan daftar malware yang terdeteksi, tab kedua adalah daftar software yang terpercaya dan otomatis masuk dalam daftar tsb pada saat proses scan, tab ketiga daftar software yang tidak diketahui status keamanannya, disini pengguna bisa memasukkannya ke dalam daftar aman jika memang dipercaya. Pada tab terakhir merupakan rangkuman dari laporan scan dengan menyertakan daftar proses yang sedang berjalan pada saat itu.



Berikutnya adalah Ignore List, Quarantine dan Update. Pada sub-tab Ignore List akan ditampilkan file – file yang dimana akan dilewatkan pada saat proses scan, sangat berguna jika Spyware Terminator salah alarm terhadap file program buatan sendiri. Quarantine, daftar file yang masuk ke dalam kurungan dimana file yang terinfeksi masih dibutuhkan sehingga akan dikurung agar tidak dihapus.

Update, memperbaharui modul program dan database deteksi Spyware Terminator. Pengguna bisa menunda untuk update modul program jika koneksi internet tidak memungkinkan untuk men-download file besar. Update database deteksi Spyware Terminator sekarang sangat ringan karena ukuran file update telah dipangkas dengan meniru metode dari Norton AntiVirus 2010, melakukan download file update seperlunya.

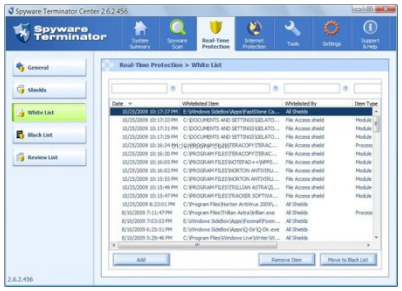


Sekarang pada tab Real-Time Protection di sub-tab General, disini pengguna dapat memilih level proteksi daru Spyware Terminator pada proteksi on-demand. Basic atau Advanced, untuk Basic sebagian besar keputusan akan otomatis di-handel oleh Spyware Terminator berdasarkan database deteksi sedangkan untuk Advanced semua keputusan akan konfirmasi berada di tangan pengguna. Sama halnya dengan sub-opsi HIPS Application Control.

HIPS Application Control, HIPS dari Spyware Terminator sama dengan COMODO Defense+ dari COMODO Internet Security.

Sebuah metode perlindungan sistem khusus untuk pengguna professional yang dimana melindungi sistem dengan memberi konfirmasi visual terhadap semua akses file program. Apapun dan kemanapun aksesnya membutuhkan konfirmasi dari pengguna apapun programnya. Jaminan 100% aman pun bisa diraih dengan metode proteksi HIPS atau biasa disebuat pertahanan proaktif (Proactive Defense), namun hanya cocok untuk pengguna professional yang mengetahui banyak kosakata software dan modul file program.

Pada sub-tab Shields, pengguna diberikan sebuah fleksibilitas dalam setiap modul proteksi Rea-Time Protection Spyware Terminator. Dimulai dari **Startup Shield** untuk memonitoring direktori startup Windows agar tidak disusupi malware yang ingin aktif pada saat Windws startup. **Services and Drivers Shield**, mengawasi daftar Windows Services dan Drivers dari perubahan yang tidak berhak. **Web Browser Add-on Shield**, mengawasi daftar add-on web browser dari akses yang tidak berhak. **File Extension Shield**, memonitoring ekstensi file beserta asosiasinya dengan program yang bersangkutan agar tidak dirubah oleh malware. **Winsock Shield**, melindungi filter Windows Socket (Winsock) dari kerusakan atau akses yang tidak berhak. **IE Setting Shield**, memonitoring setting web browser Windows Internet Explorer dari perubahan – perubahan yang tidak berhak. **System INI Shied**, melindungi file system.ini dari perubahan yang tidak berhak dimana informasi sistem file Windows tersimpan. **Host Shield**, mengawasi berbagai perubahan dari file host yang menjadi tempat penyimpanan informasi alamat IP.



Berikutnya masih dalam tab Real-Time Protection, untuk sub-tab White List adalah daftar file – file program yang dipercaya sehingga bisa berjalan tanpa perlu konfirmasi lagi. Sub-tab Black List adalah daftar dimana file program akan diblokir aksesnya oleh sistem proteksi Spyware Terminator. Dan untuk sub-tab Review adalah daftar lengkap dari apa yang telah dilakukan oleh sistem proteksi Spyware Terminator Real-Time Protection.

Selanjutnya pada tab Internet Protection disediakan 3 sub-tab, Cookies Scan untuk melakukan pemeriksaan terhadap file – file cookies yang dicurigai sebagai Tracking Cookies yang dimana memata – matai pengguna saat menjelajahi website, Favorite Scan memeriksa seluruh daftar bookmark di aplikasi web browser apakah ada website yang berbahaya. Immunize atau dalam Bahasa Indonesia yang berarti “imunisasi”, disini immunize berguna untuk pencegahan eksekusi kode berbahaya.

Tab Tools, disini developer Crawler, LLC menyediakan 4 fungsi ekstra di Spyware Terminator. System Settings untuk mengembalikan setting dari berbagai fungsi / fitur Windows ke semula yang dimana perubahan tersebut biasanya diakibatkan oleh spyware namun jika pengguna sendiri yang mengubahnya tidak perlu diset ulang. System Restore, mengembalikan kondisi sistem pada saat sebelum penghapusan malware, fitur ini memanfaatkan Windows System Restore untuk bekerja. Kalau Windows System Restore tidak aktif maka fitur System Restore dari Spyware Terminator ada gunanya, namun hal ini tidak menjadi masalah kalau pengguna mempunyai program backup yang lebih baik.
Analyze File, berfungsi untuk melakukan analisa terhadap file program apa pun, Analyze File akan melakukan analisa mendalam terhadap internal data dan security certificate sekaigus entri – entri registry. Analyze dapat digunakan untuk melakukan analisa terhadap program tak dikenal. Remove File, berguna untuk menghapus file yang dimana tidak bisa dihapus dengan cara biasa. File yang tidak bisa dihapus dengan tombol DELETE maupun SHIFT + DELETE, Remove File akan membuka kunci akses dari file tersebut lalu akan menghapusnya secara tuntas.

Lalu pada tab Settings, disini pengguna dapat melakukan pengubahan berbagai konfigurasi untuk Spyware Terminator. Dimulai pada sub-tab General, disini pengguna dapat memilih bahasa dari tampilan Spyware Terminator namun sayangnya tidak ada Bahasa Indonesia. Menampilkan icon Spyware Terminator di system tray yang dimana berguna untuk akses cepat terhadap fungsi proteksi, scan dan update. Menampilkan icon update di sistem tray pada saat Spyware Terminator melakukan update.

Pada Report Settings (tetap di sub-tab General), pengguna dapat memilih apakah mengijinkan Spyware Terminator mengirim informasi ke pihak developer untuk dianalisa. Informasi yang dikirm diantaranya adalah data aplikasi yang tidak diketahui, statistik penggunaan dan informasi catatan error Spyware Terminator. Silakan isi alamat email anda agar pihak developer bisa menghubungi anda disaat perlu.

Lalu pada sub-tab Scan Settings, Scan for Unreadable Files berguna untuk memeriksa file – file yang tidak bisa dibuka dengan program standar, biasanya file – file sistem seperti EXE dan file DLL. Scan Alternate File System,

memeriksa area Alternate File System (AFS). AFS adalah fitur dari sistem file NTFS yang dimanfaatkan oleh para pembuat spyware untuk menyembunyikan code ke dalam program atau aplikasi. Use System Restore, memanfaatkan Windows System Restore untuk menyimpan kondisi sistem disaat sebelum scan dilakukan agar kondisi sistem bisa dikembalikan saat tidak stabil. Scan Report Settings, centang Save Report History agar Spyware Terminator menyimpan catatan hasil scan dan perlindungan Real-Time Protection agar bisa dianalisa di kemudian hari, set ukuran file maksimal untuk Report History. Lalu pilih profil scan di menu utama Spyware Terminator, Fast Scan, Full Scan atau Profil buatan sendiri.

Sub-tab Real Time Protection, terdapat opsi untuk mendeteksi proses instalasi secara otomatis sehingga pada saat ingin melakukan instalasi program tertentu tidak diganggu oleh berbagai konfirmasi dari proteksi Spyware Terminator. Rebuild HIPS Database berfungsi untuk memperbaharui database HIPS Control dengan menghapus database yang lama, fungsi ini cocok digunakan pada saat jika sistem telah mengalami perubahan besar atau melakukan instalasi banyak program. Advanced Settings berfungsi untuk agar Spyware Terminator secara otomatis memberi hak akses kepada program yang dianggap aman menurut database.

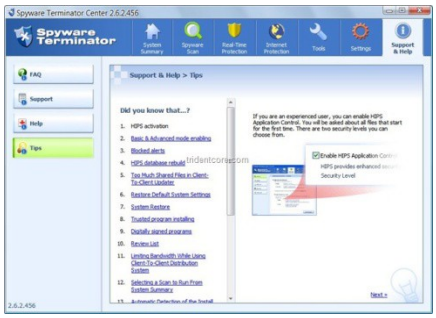
Selanjutnya pada sub-tab Scheduled Scans, disini pengguna dapat memilih berbagai konfigurasi untuk scan terjadwal dimulai dari periode setiap hari atau per minggu dan jam scan bisa set sesuai selera. Terdapat beberapa opsi diantaranya, **If I miss my scheduled time, start it immediately,** jika pengguna lupa akan jadwal scan sebelumnya. **Check Database Update before scan**, Spyware Terminator akan melakukan update sebelum proses scan dimulai agar database update tetap aktual pada saat scan dimulai. **Postpone Scheduled Scan when the computer runs in battery mode**, fungsi ini sangat berguna bagi pengguna notebook, Spyware Terminator akan menunda scan hingga notebook mendapat suplai daya dari stop kontak.

Update Settings, pada sub-tab ini semua konfigurasi update yang disediakan sangat fleksibel. Disini pengguna dapat memilih lokasi download untuk update deteksi Spyware Terminator, bisa dari server developer atau antar sesama client (Client to Client Download). Pada prakteknya yang lebih ekonomis adalah dengan menggunakan metode update sesama client karena tidak membutuhkan koneksi internet per client.

Untuk Client to Client Download tentukan konfigurasi port yang digunakan dengan mengisi area antar port yang akan digunakan sehingga metode client to client download akan menggunakan salah satu dari port yang disediakan.

Pada sub-opsi Application Update Settings disediakan 2 opsi untuk melakukan download update secara otomatis atau memberi konfirmasi mengenai update terbaru namun akan didownload setelah konfirmasi dari user. Untuk Ignore Minor Updates berfungsi untuk memprioritaskan update database sehingga untuk update modul aplikasi tidak dilakukan. Pilih koneksi internet yang digunakan, apakah koneksi langsung (modem, public WiFi) atau menggunakan proteksi proxy.

Untuk Web Security Guard dan ClamAV membutuhkan instalasi add-on Web Security Guard dan modul ClamAV. Web Security Guard melindungi user dengan melakukan instalasi add-on untuk aplikasi web browser, user akan diberi peringatan pada saat mengunjungi website yang berbahaya atau website yang tingkat reputasinya rendah. Sedangkan ClamAV adalah sebuah add-on untuk menambah proteksi antivirus di Spyware Terminator.



Terakhir adalah pembahasa fitur tab Support and Help. Pada tab FAQ pengguna dapat mencari pembahasan yang sering dihadapi oleh semua pengguna Spyware Terminator, disitu pengguna dapat mencarinya berdasarkan topik dan bisa menemukan jawaban dari masalah tersebut. Selanjutnya pada tab Support terdapat 3 pilihan opsi diantaranya **Have a Spesific Question?**, jika masalah yang dihadapi tidak ditemukan solusinya meskipun sudah eksplorasi FAQ dan Help Index, pengguna dapat mengunjungi forum Spyware Terminator untuk bertanya disana dan menunggu jawabannya dari tim Spyware Terminator atau member lain. Untuk opsi yang kedua, **Take a Tour Spyware Terminator Support Guide**, pada link yang disediakan pengguna akan dibawa ke sebuah halaman web di website Spyware Terminator. Disitu pengguna dapat mengeksplorasi berbagai topik pertanyaan dan panduan dalam berbagai masalah saat menggunakan Spyware Terminator. Jika mempunyai saran atau kritik pengguna bisa menggunakan opsi yang ketiga yaitu **Send us a Feedback**, pada link yang disediakan pengguna bisa memberi sebuah saran, kritik atau testimonial kepada tim developer Crawler, LLC.

Lalu pada sub-tab Help, terdapat 2 opsi yang sebenarnya sama namun hanya berbeda di metode aksesnya saja. Online Help dan Offline Help, disini tergantung dari pengguna saja untuk memilih yang mana, namun untuk Offline Help diharuskan untuk mendownload kontennya agar bisa diakses tanpa harus terhubung dengan internet.

Lalu pada sub-tab terakhir yaitu Tips, disini pengguna dapat melihat berbagai tips yang disediakan oleh Spyware Terminator pada setiap fiturnya. Namun sayangnya hanya bisa diakses pada saat terhubung dengan internet.

Dibawah ini adalah tampilan dari konfirmasi visual Spyware Terminator, untuk yang kiri adalah tampilan basic dari konfirmasi visual, pengguna tinggal memilih **Allow** atau **Deny** dari program yang meminta hak akses ke program/modul lain. Lalu untuk yang kanan khusus untuk pengguna professional karena bisa memilih berdasaran sumber program beserta proses-proses dibawahnya dan modul – modulnya sehingga tidak perlu banyak konfirmasi.

Lalu dibawah ini adalah tampilan konfirmasi dari Spyware Terminator pada saat mendeteksi sebuah malware, pengguna bisa melihat detail dari malware tersebut dan juga memilih periode waktu untuk durasi blokadenya.