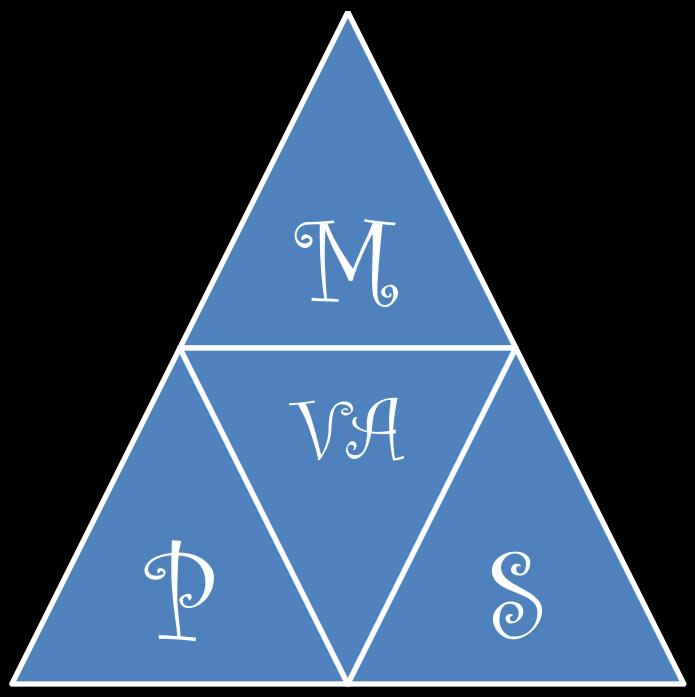


وناک و آوناک دتکشن مالور اسکنر

نگارش MPS

چگونه کار می کند ؟

U0vd Security Inc 2008 (C)

وناک و آوناک ابزاری امنیتی است برای شناسایی تهدیدات ناشناخته در سیستم عامل ویندوز.

این ابزار با استفاده از تکنولوژی به نام MPS توانایی شناسایی تهدیداتی نظیر ویروس ، روتکیت ، تروجان ، اسپای ورها و.... را دارا می باشد.

در حقیقت وناک و آوناک سعی دارد به شما نشان دهد که کدام یک از برنامه های اجرا شده در ویندوز می توانند تهدید کننده باشند و به سیستم شما صدمه بزنند.

وقتی که این ابزار را برای اولین بار اجرا کردید قبل از هر اقدامی ابتدا برنامه های سیستم خودتان که بر روی ویندوز نصب شده را به سیستم تراست وناک معرفی کنید.

برای انجام این کار تنها کافی است بر روی نام برنامه در بخش Processes دبل کلیک کرده و در منو های جاری گزینه Add Trust Process را انتخاب نمایید.

نکته مهم : از ثبت کردن برنامه های ناشناخته جدا خوداری نمایید .

برنامه های که برروی سیستم شما نصب می شوند شامل ابزارهای کاربردی مانند فایروال ، وب سرورها ، آنتی ویروسهای دیگر ، ابزارهای اینترنتی ، ابزارهای ملتی مدیا ، مسنجرها اینترنتی و موارد دیگر شامل برنامه های که شخصا روی دستگاه خودتان نصب کرده اید می باشند.

وناک و آوناک برنامه هایی را که شما به مود تراست ارسال می کنید را به رنگ سبز نشان می دهد ، همچنین برنامه های سیستمی نیز با رنگ سبز نشان داده خواهند شد.

در بخش Processesگاهی برخی از پروسه ها (برنامه های اجرایی) چه آنهایی که تراست هستند و چه بقیه موارد به رنگ بنفش نشان داده می شوند ، این رخداد در زمانی پیش خواهند آمد که وناک و آوناک قصد دارد به شما بگوید که برنامه مورد نظر از تکنیکی خاص استفاده می کند و این تکنیک ها شامل موارد زیر می شود:

شما این تکنیک ها را در بخش Error type مشاهده خواهید کرد

- Valid Processes (Green)
- Sensitive Threat (Red)
- Parent PID Isn’t Valid (Magenta and Red)
- The Program hasn't any GUI (Magenta and Red)
- (No Executable Path) Sensitive threat (Yellow)
- File Signature Changed! (Yellow)
- EProcess Is Null (Yellow)

چه زمانی رخ می دهند ؟

حالات تکنیکی که در بالا به آنها اشاره شده اند در زمانی رخ می دهند که عوامل زیر اتفاق بیفتد

Valid Processes (Green)

- زمانی که یک پروسه ولید هست یعنی پروسه شناسایی شده است (یعنی برنامه به نحوی درستی اجراشده)

Sensitive Threat (Red)

- زمانی که یک پروسه از روش جعل نام برای مخفی ماندن از دید کاربر بر روی سیستم شما اجرا شده باشد به عنوان مثال ویندوز از نام SVCHOST برای عملیات سیستمی خود استفاده می کند و امکان دارد برخی از ویروس ها از این نام برای خود استفاده کنند تا برای کاربران قا نونی به نظر بیایند ، وناک هر وقت جعل نامی صورت گیرد آن را با این عامل به شما نشان خواهد داد.

Parent PID Isn't Valid (Magenta and Red)

- (یعنی برنامه توسط عوامل درستی اجرا شده مثلا شما آن را اجرا کردید یا توسط یکی از برنامه هایی که شما به سیستم شناسایی کرده اید ، اجرا شده است)
- زمانی که یک برنامه (پروسه ، مثلا ماشین حساب) به وسیله **کلیک کردن** شما اجرا می شود شما آن را اجرا کرده اید و این برنامه جز برنامه های قانونی است ، وناک و آوناک برنامه هایی را که برنامه های جاری را اجرا کرده اند را چک می کند (برنامه پدر) و اگر ساختار آن به صورت یک برنامه قانونی بود با رنگ بنفش و اگر تهدید کننده بود با رنگ قرمز آن ها را نمایش می دهد.
- لازم به ذکر است برنامه هایی را که به واسطه Windows Explorer یا Services.exe اجرا شده باشند در محدوده ی نرمال قرار می گیرند (یعنی به رنگ سفید)

The Program hasn't any GUI (Magenta and Red)

- وناک ساختار GUIرا چک می کند (واسط کاربری ویندوزی) و اگر شبیه به یک برنامه نرمال باشد به رنگ بنفش و در غیر این صورت با رنگ قرمز نشان می دهد.

(No Executable Path) Sensitive threat (Yellow)

- برنامه مسیر اجرایی ندارد – برخی از آنتی ویروس ها و برنامه های سیستمی می توانند شامل این عامل باشند ،همچنین برخی از روتکیت ها. پس تنها وجود آن نشان بر تهدیدکنندگی نیست.

File Signature Changed! (Yellow)

- امضا فایل تغییر کرده است.

EProcess Is Null (Yellow)

- این عامل در حقیقت مربوط به بخش هسته ویندوز و ساختار پروسه ها می باشد ، برنامه هایی که فاقد یک ساختار ویندوزی صحیح می باشند به این شکل نمایش داده می شوند.

گاهی اوقات برخی از تولید کنندگان محصولات امنیتی برای محافظت از برنامه خودشان دست به این ساختار می زنند.

در سیستم عامل ویندوز ویستا نیز برخی از پروسه های سیستمی به این صورت تعریف شده اند.

Hidden Process (Red)

- اگر پروسه اجرا شده از تکنیک های روتکیتی برای مخفی شدن از دید آنتی ویروسها یا برنامه های امنیتی ویندوز مانند Task Managerمخفی شوند با این عامل توسط وناک شناسایی می شوند
- اگر برنامه مورد نظر در محدوده ی تراست باشد با 2 عامل منفی و اگر نباشد با 3 عامل منفی مشخص می شود .

The MPS (Main Protection System)

MPSچیست ؟

MPS تکنولوژی جدیدی است برای تشخیص ویروس های ناشناخته کامپیوتری در سیستم ویندوز.

این تکنولوژی با استفاده از یک مدل امنیتی شروع به تحلیل برنامه ها (پروسه) کرده و آن ها را از نظر تهدید کنندگی درجه بندی می کند.

این تحلیل ها براساس دسترسی پروسه ها به منابع سیستم عامل صورت می گیرند مانند سرویس ها ، درایورها ، کلید های رجیستری و بسیاری از قابلیت های امنیتی دیگر، در حقیقت MPSسعی دارد به شما فعالیت برنامه های تهدید کننده را نشان دهد.

نکته مهم : زمانی که شما MPSرا Start می کنید چنانچه پروسه تهدید کننده ای وجود داشته باشد آن را درجه بندی می کند ، برای پروسه های عادی (غیر تراست) اگر این میزان درجه بندی به عدد 3 برسد پروسه تهدید کننده به حساب می آید و برای پروسه های (تراست شده) اگر این میزان به عدد 4 برسد تهدید کننده به حساب می آید و بسته به تنظیمات برنامه با آن برخورد خواهد شد.

MPS تکنیک های امنیتی زیر را پشتیبانی می کند:

Sensitive Threat (2 rates)

Parent PID Isn't Valid (Magenta 1 rate and Red 2 rates, if Process is valid 1 rate)

The Program hasn't any GUI (Magenta 1 rate and Red 2 rates, if Process is valid 1 rate)

(No Executable Path) Sensitive threat (2 rates, if process is valid or invalid)

File Signature Changed! (1 rates if Process is valid)

EProcess Is Null (1 rate, if process is valid or Invalid)

Windows Handles and GDI and User Interface Is Not Enough (1 rate, if process is Invalid)

Hidden File Attribute (1 rate, if process is valid or invalid)

Hidden Process (Rootkits techniques, 2 rates, if process is valid and 3 rates, if process is invalid)

Information Problem (1 rate, if process is valid or Invalid)

- زمانی نمایش داده می شود که یک فایل حاوی مشخصات تولید کننده نباشد ،شامل درایور ها ، DLLها و درایورهای تحت هسته
- Same Executable Folder (show with Magenta color)

Process Calls the other Executable File (1 rate, if process is Invalid)

- زمانی که یک پروسه برنامه دیگری را فراخانی کند و سعی در زنده نگه داشتن برنامه مورد نظر داشته باشد (این تکنیک بیشتر مورد توجه ویروس نویسان بوده تا سعی کنند برنامه ویروسی آن ها به فعالیت خود ادامه دهد)

A Startup Service (1 rate, if process is Invalid)

- A Service but Shutdown (0 rate, if process is valid)

ICMP packets is too much (show with Magenta color)

- ICMP packets is very too much (show with Red color)

Registry Startup (1 rate, if process is Invalid)

Same MD5 (1 rate, if process is Valid or Invalid)

اختارهای سراسری برنامه

Registry Startup keys (only invalid Keys; this ability check Process path and registry Keys)

این مورد در زمانی پیش می آید که برخی از پروسه ها که شما آن ها را به مود تراست ارسال **نکرده اید** قصد دارند در شروع مجدد ویندوز دوباره اجراشوند. (هر کدام از این برنامه ها را که قصد دارید از اجرای مجدد حذف کنید فقط کافیست به بخش Startup Filesرفته روی نام آن کلیک کرده و سپس بر روی گزینه Delete Selected کلیک کنید تا پاک شوند)

DLL Information Problems

- Same Executable Folder (show with Magenta color)

Hooks contain:

- DLL Hooks
- Device Driver, Kernel Driver and Services Hooks
- SSDT Hooks (System Service Descriptor Table)

Invalid Running Services

- پروسه های را که در مود تراست **قرار ندارند** و در حال حاضر در سیستم اجرا شده اند را به رنگ **بنفش** نمایش می دهد
- نکته مهم : زمانی که پروسه ای را به مود تراست ثبت می کنید به صورت اتوماتیک سرویس های مربوط با آن نیز به مود تراست ارسال می شوند.

Malicious Access

- زمانی به شما اختار می دهد که یک برنامه مانند بکدور بخواهد اطلاعات سیستم شما را به بیرون انتقال دهد.
- نکته مهم : پروسه Cmd.exe را به محدودهی تراست **ثبت نکنید** بدان علت که امکان تشخیص بکدور ها را از وناک صلب می کند

Kernel Driver, Device Driver, Services and Windows Explore entries

- وناک درایور ها و سرویس های اضافه شده و حذف شده را به شما نمایش می دهد (به بخش تنظیمات مراجعه شود)
- همچنین به شما DLL های اضافه شده Windows Explorer را نمایش می دهد.
- وناک خصوصیات فایل ها و پروسه های در حال اجرا را به شما نشان می دهد که شامل نام تولید کننده ،اطلاعات فایل و زمان ایجاد آن بر روی سیستم شما می شوند.
- اگر درایور تحت هسته ای خصوصیات و اطلاعات تولید کننده نداشته باشد با رنگ قرمز نمایان می شود.
- اگر DLL به فضای آدرس دهی برنامه Windows Explorerاضافه شوند وناک آن را با عنوان This is adding New نمایش می دهد و همچنین آن را به رنگ بنفش در می آورد.
- سرویس های درست و قابل اطمینان به رنگ **سبز** نمایش داده می شوند.
  - سرویس های که توضیحات تولید کننده مناسبی نداشته باشند با رنگ بنفش نمایش داده می شوند.
  - سرویس های که فایل آن ها اطلاعات تولید کننده نداشته باشند با رنگ قرمز نمایش داده می شوند.
  - سرویس های غیر تراست با رنگ **زرد** نشان داده می شوند.
- سرویس ها و درایور هایی که در 20 روز آخر از زمان جاری به سیستم اضافه شده باشند برای آگاهی دادن به شما از وجود آنها با رنگ بنفش نشان داده می شوند.
- شما می توانید MPSرا به گونه ای پیکربندی کنید که تنها سرویس ها و درایور های اضافه شده را نمایش دهد ، برای انجام این منظور از منوی Main Settingsگزینه Main Protection System (MPS) Settings را انتخاب کرده و گزینه show only added modules for MPSرا چک دار کنید.

چگونه می توانیم ویروس ها را به کمک وناک شناسایی کنیم ؟

اگر مراحل زیر را دنبال کنید می توانید به کمک وناک فایل های تهدید آمیز مانند ویروس ها ، کرم ها و روتکیت ها را شناسایی کنید

1. پروسه های برنامه های کاربردی را به محدوده ی تراست ببریم تا وناک آن ها را به عنوان تهدید در نظر نگیرد.
2. هارد درایو سیستم خود را با کمک ابزار جانبی Threat Files که در منوی Threat Files وجود دارد به طور کامل اسکن نمایید (به صورت دوره ای بسته به نیاز شما مثلا هفته ای یا روزانه)
3. MPSرا استارت می کنیم.
4. نتایجی که از آنالیز برنامه ها و پروسه ها نشان داده می شود را آنلایز می کنیم و دنبال تهدیدات می گردیم (در وناک به صورت استاندارد اگر پروسه ای تهدید آمیز باشد با درجه رنگ قرمز نمایش داده می شود و عدد تهدید کنندگی هم معمولا 3 و بیشتر خواهد بود)
5. پورت های اینترنتی را چک می کنیم (برنامه های غیر تراست با رنگ زرد مشخص می شوند)
6. کلید های رجیستری را نیز چک می کنیم.
7. نتایج را تحلیل می کنیم و دنبال عوامل تهدید کنند می گردیم و برای پاک سازی آنها اقدام می کنیم.

نکته مهم : شما می توانید با استفاده از مکانیزم ویژه در وناک آن را به صورتی پیکربند کنید که به شکل خودکار تمامی موارد تهدید کننده را به حالت فریز نگاه دارد ولی برای پاکسازی آن ها حتما باید به صورت دستی آن را از منوی Debugانجام دهید.

برای این که بتوانیم با دقت برنامه های نصب شده در سیستم خودتان را شناسایی کنید باید مسیر برنامه های اجرا شده را به دقت به خاطر داشته باشید و در زمانی که برنامه ها درحال اجرا هستند آن ها را به محدوده ی تراست بفرستید .

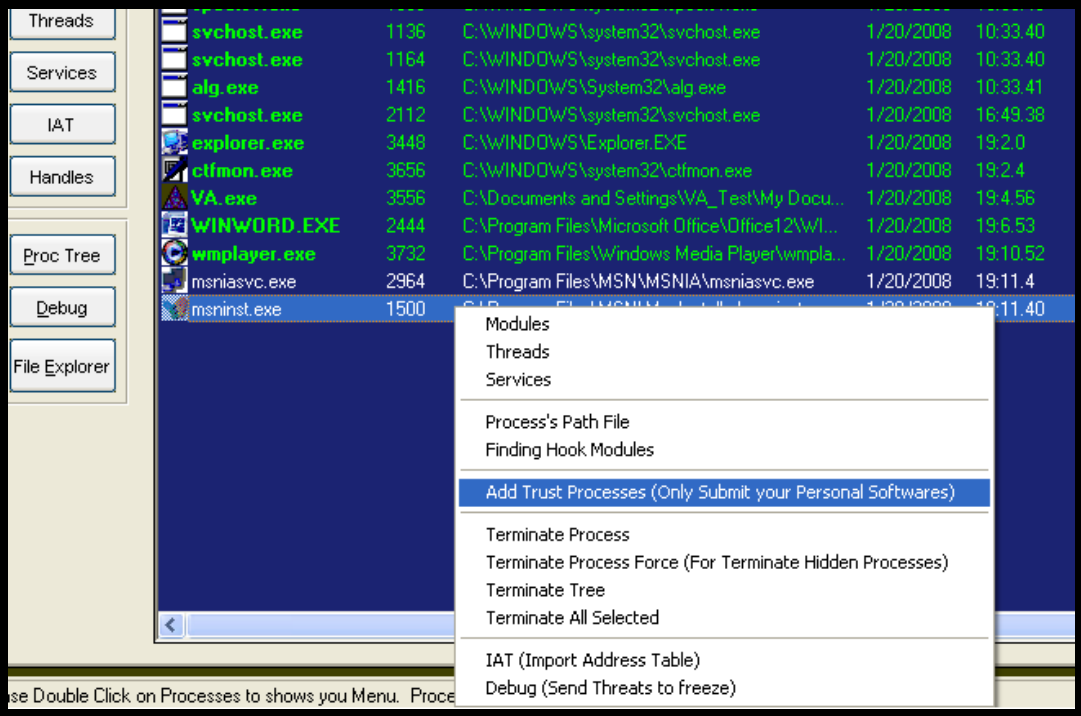
از ثبت کردن برنامه های قرمز رنگ یا مشکوک جدا خوداری نمایید.

برای این که مسیر فایل های اجرای را به دقت پیدا کنید در ابتدا بر روی Startویندوز کلیک کنید وسپس برروی نام برنامه ای را که می خواهید آن را به مد تراست ارسال کنید کلیک کنید تا اجرا شود ، سپس دوباره برروی همان برنامه در منوی استارت رفته این بار کلیک راست را بزند و سپس گزینه Propertiesرا انتخاب کنید تا مسیر اجرای فایل را دقیقا به شما نشان دهد .

پس از آن به صفحه Processesدر وناک رفته و برروی همان نام و مسیر برنامه اجرا شده دوبار کلیک کرده واز منوی های مربوطه گزینهadd trust process را انتخاب نمایید.

نکته مهم : از ثبت کردن برنامه های ناشناخته خوداری نمایید و همچنین از ثبت کردن پروسه Cmd.exeخوداری نمایید.

روش ثبت کردن یک پروسه قانونی در شکل به تصویر کشیده شده است.



اسکن کردن فایل های هارد دیسک

در زمانی که شما قصد اسکن کردن هارد درایو خودتان را دارید گزینه های متفوتی برای انجام این کار وجود دارد.

نکته مهم : وناک وقتی هارد شما را اسکن می کند به دنبال فایل هایی می گردد که پراکندگی زیادی را دارند و سعی دارند با استفاده از تکنیک های فریب دهنده در سیستم شما ثبت شوند ، مثال واضح آن فایل هایی هستند که در ریشه درایوهای شما به صورت استارت آپ اجرا می شوند ، وناک این فایل ها را شناسایی می کند و در اختیار MPSقرار می دهد و از مکانیزم MD5برای شناسایی دیگر تهدیدات نظیر آن استفاده می کند.

در زمان اسکن کردن گزینه انتخاب شده به صورت default گزینه Quick Scan می باشد ، این گزینه به صورت خودکار به دنبال فایل هایی می گردد که در مکان های مهم ویندوز و هارد جای دارند مانند فولدر های اصلی ویندوز ، فولدرها و فایل های کاربر جاری ، و فایل هایی که قصد دارند به نحوی اجرای مجدد شوند.

در زمانی که شما MPSرا استارت می کنید اگر پروسه ای با یکی از این فایل های اسکن شده یکسان بودند و قصد آسیب رسانی یا به نحوی مخفی ماندن از چشمان شما را داشته باشند وناک پیغام Same MD5 را برای آن صادر می کند.

Binder Detection

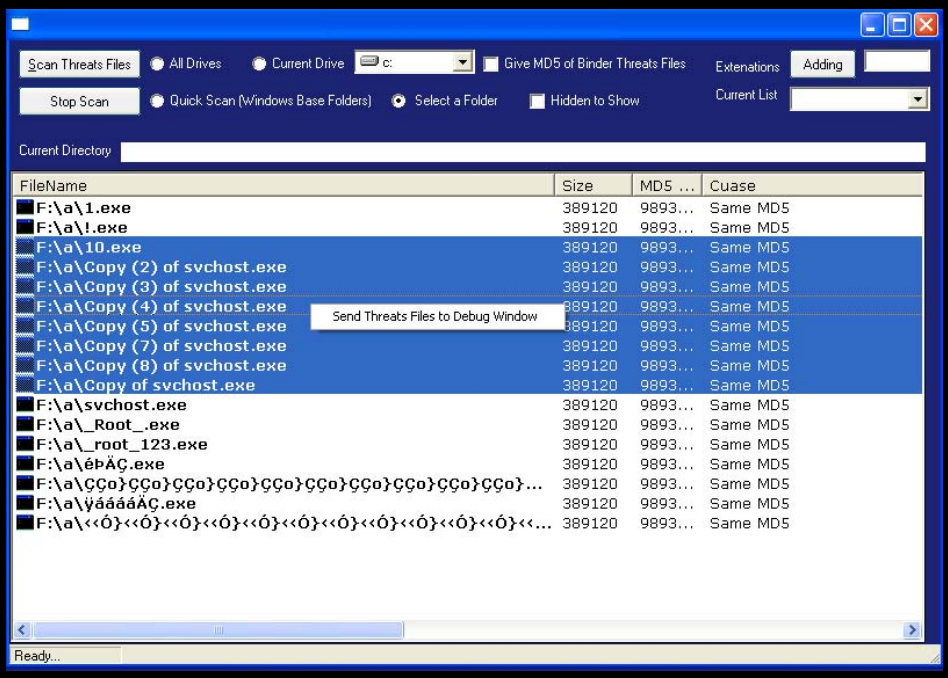
برخی از فایل های ویروسی وجود دارند که به فایل های عادی می چسبند و به همراه آن ها اجرا می شوند وناک توانایی شناسایی این موارد را نیز داراست و آن را به پیغام Binder Detection نمایش می دهد.

نکته مهم : تمامی فایل که پیغام Binder Detection را دارا می شوند ویروس یا تهدید نیستند چون بسیاری از فایل های Self Extractor نیز از همین تکنیک استفاده می کنند (فایل های Setupیا Installبرنامه و نظایر آن ها)

پس نگرانی در ارتباط با تشخیص آن ها وجود ندارد ،اگر میزان تهدید کنندگی آن ها شبیه ویروس باشد وناک آن را به شما نشان خواهد داد یا به نحوی دنبال پروسه آن ها در سیستم اجرایی ویندوز می گردد.

وناک به صورت اتوماتیک تمامی MD5 (امضای فایل) را به شما نشان خواهد داد تا از پراکندگی فایل ها در مکان های مهم کاملا آگاه شوید.

Threat files به صورت عادی فرمت های SCR, EXE, PIF, COM, CMD را جستجو می کند.



Start MPS

زمانی که شما MPSرا استارت می کنید این سکریتی مدل در ابتدا به دنبال منابع استفاده شده برنامه های اجرا شده در سطح سیستم می گردد که شامل مسیر اجرایی فایل ها ، PID، کلیدهای رجیستری ، DLLها ، پورت های اینترنتی و سرویس های وابسته به آن پروسه می شود.

شما همچنین می توانید MPSرا به گونه ای پیکربندی کنید که هیچ گونه واسط کاربری نداشته باشد و درپس زمینه سیستم به کار خود ادامه دهد ، همچنین تهدیدات به وجود آمده را به صورت خودکار به حالت فریز (Freeze) ارسال می کند.

در صورتی که شما بخواهید وناک را به حالت مرعی برگردانید تنها کافی است کلیدهای ALT + V را با هم بفشارید.

نتایج MPS

اگر یک پروسه در وناک با مقدار 3 و به صورت invalid نمایش داده شده امکان آن وجود دارد که این پروسه یک پروسه تهدید آمیز برای سیستم شما باشد ، برای این که کاملا از این بابت اطمینان حاصل کنید تنها کافی است برای پیدا کردن دلایل آن به بخش های انتهایی پروسه مورد نظر مراجعه کنید (منظور نتایجی است که MPS به شما نشان می دهد)

نکته مهم : بار دیگر متذکر می شوم که تمامی پروسه هایی که مربوط به برنامه هایی هستند که شما آن ها را برروی سیستم خود نصب کرده اید به **مد تراست** ارسال کنید.

زمانی که MPSیک پروسه را با عدد 4 یا بیشتر نمایش داد می توانید اطمینان حاصل کنید که این پروسه یک پروسه تهدید آمیز می باشد یعنی امکان آن که این پروسه بتواند به سیستم شما صدمه بزند زیاد می باشد ، اگر تمامی برنامه های کاربری خود را به سیستم تراست وناک برده اید می توانید با نگاه کردن به عواملی که سبب رخ دادن چنین حالتی شده اند تشخیص دهید که این فایل یک برنامه تهدید کننده یا به نحوی یک ویروس کامپیوتری می باشد.

خوشبختانه MPSبا استفاده از روشی می تواند به صورت خودکار از فعالیت این گونه برنامه ها جلوگیری کند و پس از این که دریافت این پروسه یک پروسه تهدید آمیز است آن را به حالت فریز(Freeze) می برد تا نتواند به سیستم شما بیش از این آسیب برساند ، برای استفاده از این قابلیت تنها کافی است send threat to freeze (debug) را چک زده و برروی دکمه Start MPSکلیک کنید تا با استفاده از زمان سنج وناک این عمل به صورت خودکار انجام شود.

این تکنیک اگر تشخیص دهد که پروسه ای به حالت روتکیت برروی سیستم شما نصب شده است بلافاصله آن را از فضای سیستم عامل بیرون می برد .

زمانی که وناک یک پروسه را به صورتی به حالت فریز برده و شما تشخیص داده اید که آن یکی از برنامه های شما بود تنها کافی است آن را از منوی Debug و Debug Programs to Freeze انتخاب و برای آزاد سازی برروی release کیلک کنید.

همچنین اگر تمایل دارید این فایل ها به صورت کامل از روی سیستم شما پاک شوند برروی Erase Checked Filesکلیک کنید تا به صورت کامل از روی سیستم شما پاک شوند.

Type	Name	Path Files					
Processes							
DLL	C:\Pro...	C:\Program Files\MSN\MsnInstaller\...	PID = 1500	DLL Information Pr...			
Hooked DLL	C:\Pro...	C:\Program Files\Microsoft Office\Off...	PID = 2472	SetUnhandledExce...	© 2006 Microsoft Corporation. A...	FV = 12.0.4518.1014	PV = 12.0.4518.0
Hooked DLL	C:\Pro...	C:\Program Files\Microsoft Office\Off...	PID = 2472	SetUnhandledExce...	© 2006 Microsoft Corporation. A...	FV = 12.0.4518.1014	PV = 12.0.4518.0
Registry	C:\Pro...	HKEY_CURRENT_USER\Software\Micro...	key Nam...				
Process (3)	cmd.exe	C:\WINDOWS\system32\cmd.exe	PID = 3660	EP = 81571DA0	Graphical windows is not enough	Windows Handles and GDI and User Interfac...	Same MD5
Kernels							
Kernel	dump_...	\SystemRoot\System32\Drivers\dum...	Driver Inf...				
Kernel	dump_...	\SystemRoot\System32\Drivers\dum...	Driver Inf...				
Kernel	IsDrv1...	\SystemRoot\System32\Drivers\IsDrv...	Driver Inf...				
Driver	UIUSys	C:\WINDOWS\system32\drivers\UIUSy...	Kernel Dr...	Device Driver Infor...			
Windows Explorer	PID = 3...	DLLs Count = 143	Added C...				
Explorer DLL (Add)	IMM32....	C:\WINDOWS\system32\IMM32.DLL	Microsoft...	FV = 5.1.2600.2180	Create Time = 2004/9/1		
Explorer DLL (Add)	msctfi...	C:\WINDOWS\system32\msctfime.ime	Microsoft...	FV = 5.1.2600.2180	Create Time = 2004/9/1		
Explorer DLL (Add)	ATL80....	C:\WINDOWS\WinSxS\x86_Microsoft.V...	Microsoft...	FV = 8.0.-14809.762	Create Time = 2006/12/1		

چک کردن فعالیت های برنامه و پیغام های آن

یک آپشن در پنجره MPSوجود دارد به نام Show all Results، این آپشن به شما کمک می کند تا تمامی برنامه ها را به دقت آنلایز و بررسی کنید.

شما می توانید جزعیات کلی برنامه اجرا شده را که شامل : پروسه پدر ، زمان اجرا ، مسیر اجرایی فایل ،دستگیره پروسه و ولید بودن یا نبودن و همچنین پیام ها را مشاهده کنید.

علت و معلول چیست و چگونه می توانیم به واسطه آن ویروس ها را شناسایی کنیم ؟

این یک تکنیک بسیار ساده می باشد تا به واسطه آن شما می توانید یک تهدید خطر ناک را به راحتی شناسایی کنید ، تهدیدهایی شبیه به worms یا Malware (Malicious Software) (ابزارهایی که برای اهداف بد نوشته می شوند) .

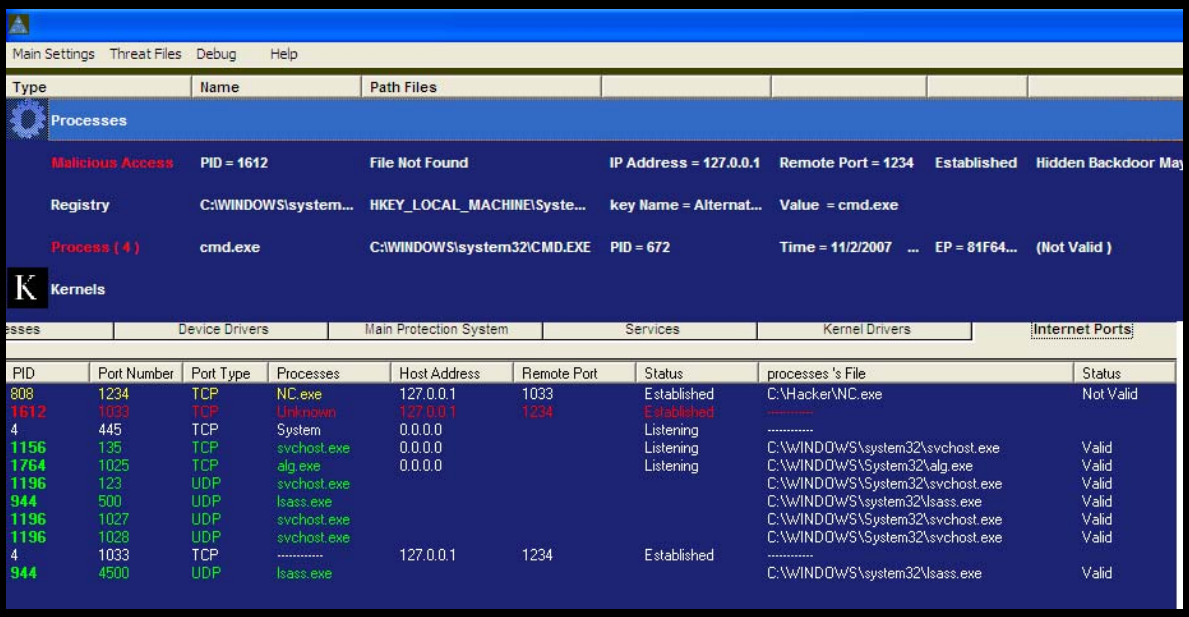
شما می توانید برخی از این عوامل را در زیر مشاهده کنید:

- این تکنیک در حقیقت یک نوع یافتن علت و معلول می باشد تا به واسطه آن بتوانید راه کارهای امنیتی را فرا بگیرید.
- به عنوان مثال چرا یک برنامه واژه پرداز شبیه به Notepadباید به اینترنت یا شبکه خارجی دسترسی داشته باشد ؟
- چرا یک پروسه ناشناخته باید دارای یک سرویس یا یک کلید رجیستری استارت آپ باشد ؟

نکته مهم : بار دیگر متذکر می شویم اگر در ارتباط با برنامه های نصب شده برروی سیستم خودتان اطلاعات کافی ندارید از راهبر سیستم خود(کسی که دستگاه را برای شما فراهم کرده) کمک بگیرید تا به شما در شناسایی برنامه های قانونی کمک کند.

- یک پروسه مخفی Hidden Processesیک تهدید بلقوه به حساب می آید زیرا سعی دارد از دید سیستم عامل و ما خود را پنهان کند.
- چرا زمانی که یک برنامه قانونی را اجرا می کنید ، برنامه مورد نظر در سیستم وناک با پیغام Parent PID Isn't Validمشاهده می شود ؟ (برخی از ویروس ها با اضافه کردن تکنیک های این چنین سعی دارند خود را به همراه برنامه شما اجرا کنند تا بتوانند برای همیشه بر سیستم وفایل های شما دسترسی داشته باشند).

فعالیت های پورت ها اینترنتی



برای این که به دقت برنامه هایی را که در سیستم شما دسترسی به فضای خارجی (اینترنت و یا شبکه های همجوار) شناسایی کنید می توانید به تب internet ports مراجعه نمایید تا به راحتی آن ها راشناسایی کنید.

برنامه هایی که ناشناخته می باشند با رنگ زرد نمایش داده می شوند.

برنامه های مجاز با رنگ سبز نمایش داده می شوند.

برنامه هایی که به رنگ قرمز مشاهده می کنید دارای 2 عامل می توانند باشد که یکی از آن ها یک خطر بلقوه و دیگر یک نمایش از یک فرآیند سیستمی می باشد.

برخی از بکدورها (یک روش در هک کردن) با استفاده از یک تکنیک قابل تشخیص سعی در انتقال اطلاعات از سیستم شما به سیستم خودشان دارند ، این گونه موارد در زمانی که ارتباط با مقصد (نفوذگر) برقرار باشد با رنگ قرمز نمایش داده می شود.

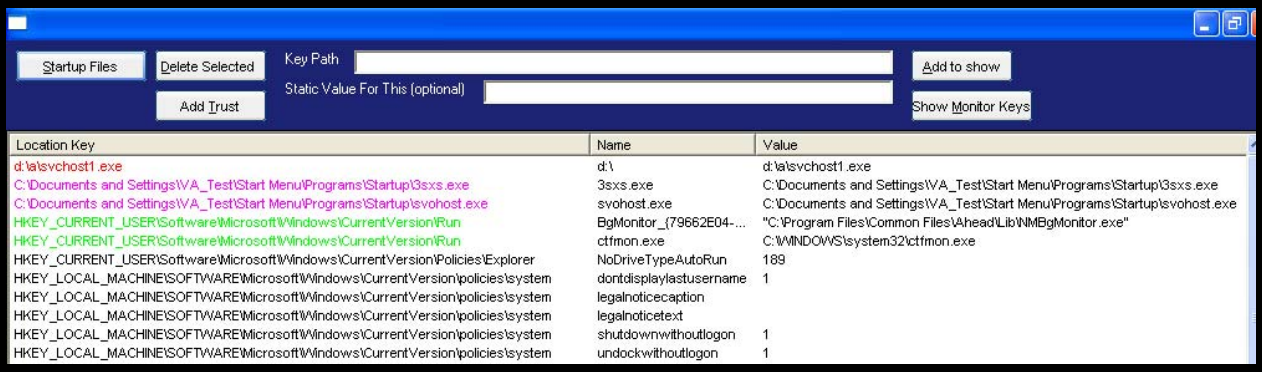
همانظور که در شکل بالا ملاحضه می فرمایید برنامه NC.exeیک برنامه ناشناخته می باشد و بنابراین با رنگ زرد نمایش داده می شود ، در خط پایین تر آن که با رنگ قرمز نمایش داده شده پروسه ای با عنوان Unknown وجود دارد که در بخش Statusآن عبارتی با عنوان Established نمایان است که نشان دهنده یک ارتباط غیر مجاز و تهدید کننده می باشد.

برنامه هایی که کلید های رجیستری استارت آپ دارند

این ابزار به شما نشان می دهد که کدام یک از برنامه های در رجیستری تغییراتی را اعمال کرده اند که به واسطه آن ها امکان اجرای مجدد آن ها میسر خواهد شد.

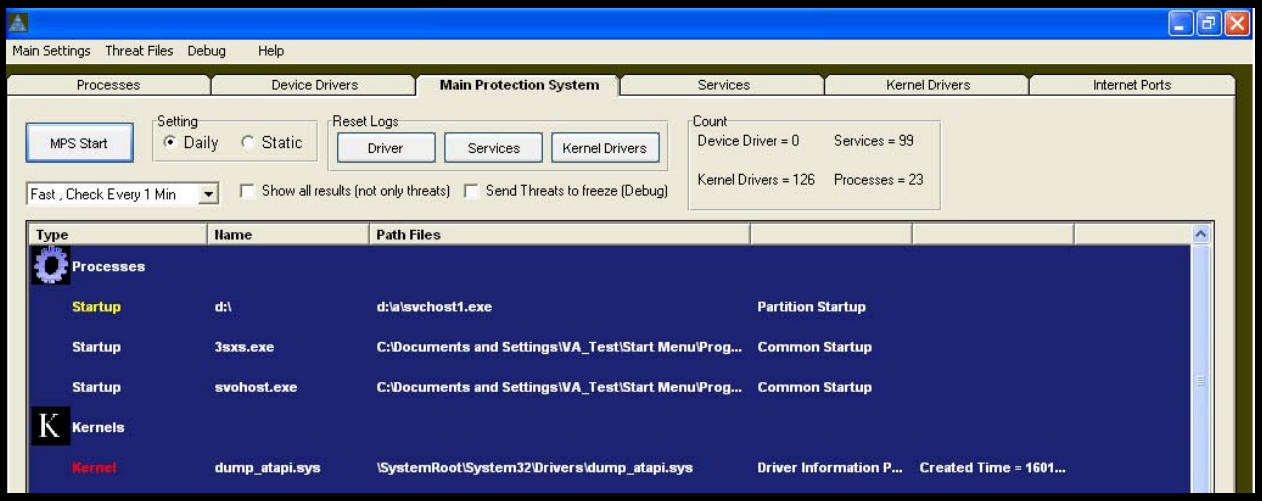
شما می توانید برنامه هایی را که نیاز به اجرای مجدد آن ها نمی بینید را پاکسازی کنید (منظوز کلید رجیستری آن ها می باشد ، نه خود برنامه)

مانند همیشه این ابزار با رنگ های متفاوت تهدیدات را مشخص می کند ، رنگ بنفش یعنی پروسه ناشناخته می باشد ، رنگ قرمز یعنی تهدید آمیز و رنگ سبز مجاز می باشد.



تکنولوژی MPSبه صورت اتوماتیک کلید های ناشناخته رجیستری را به شما نشان می دهد .

MPSبه صورت اتوماتیک به برنامه هایی که دسترسی به رجیستری دارند یک نمره منفی می دهد.



آنالیز نهایی برای پیدا کردن تهدیدات واقعی

زمانی که MPSنتایج نهایی خود را به شما نشان داد در ابتدا به دنبال برنامه های ناشناخته بگردید و آن ها را از نظر تهدیدکنندگی وناک بررسی کنید ، بیشتر برنامه های تهدیدکننده با رنگ قرمز نمایش داده می شوند ، سعی کنید برنامه هایی که بیشتر اوقات از آن ها استفاده می کنید به مد تراست ببرید تا به راحتی یک برنامه قانونی را از غیر قانونی تشخیص دهید.

کلام آخر

به خاطر داشته باشید هیچ محصول امنیتی در دنیا وجود ندارد که بتواند امنیت سیستم ها را به صورت 100% تضمین کند و وناک و آوناک نیز جزعی از این محصولات می باشد .

همیشه نکاتی است که از چشم های ما (به عنوان تولید کنند) و شما (به عنوان کاربر) پنهان می شود به عقیده ما علت آن ضعف در سیستم ها و تکنولوژی ها نیست بلکه علت آن فاکتورهای نا امن انسان می باشد .

شما می توانید با داشتن یک تفکر دفاعی خود را از بیشتر تهدیداتی که امروزه وجود دارند دور کنید ، این نکته را به خاطر داشته باشید که این انگشت کلیک کننده شماست که به شما امنیت می بخشد ، پس قبل از هر کلیک خوب فکر کنید.

ما سعی کردیم این محصول را به گونه ای طراحی کنیم تا همه عوامل و نکات امنیتی را در نظر بگیرد ، چنانچه نکاتی هستند که نیاز به انتقال آن ها به ما دارید لطفا کوتاهی نفرمایید .

موفق و امن باشید

Website: www.u0vd.org

Usenet: http://groups.yahoo.com/group/anti_malware

- ✓ Help Us

Your idea about VA\MPS Please sends

- ✓ Idea AT u0vd.org

Any information about Products and Security tools

- ✓ Info AT u0vd.org

Contact with manager Please sends

- ✓ Nima AT u0vd.org