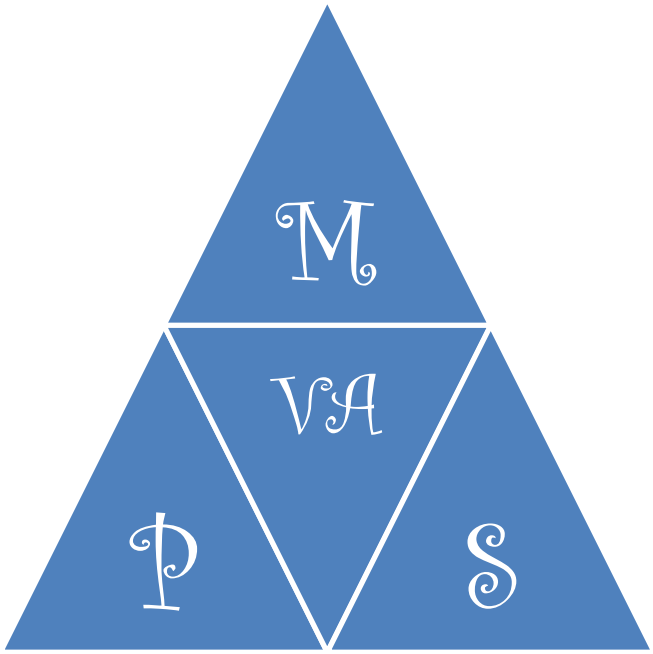
U0vd Security Inc 2008 (C)



Venak & Avenak Detection Malware Scanner

MPS Edition

چه نوع تهدیدهایی را می تواند تشخیص دهد ؟

Contents

About Venak & Avenak Detection Malware Scanner (MPS Edition)

- What is VA Detection Malware Scanner?
- What is the MPS?

MPS capabilities

Support viruses and Rootkits technique

None support things

VA's New Technologies

Help

- Product's Website (Support and Updating)
- Contact us

U0vd Security Inc 2008 (C)

About Venak & Avenak Detection Malware Scanner (MPS Edition)

- **What is VA Detection Malware Scanner**?

وناک و آوناک یک محصول امنیتی است برای شناسایی ویروس های کامپیوتری ناشناخته ، این محصول با استفاده از تکنولوژی MPS یا Main Protection System توانایی تشخیص تهدیدات ناشنا خته را دارا می باشد.

وناک سعی می کند به شما نشان دهد که کدام برنامه قانونی و کدام برنامه ها خطرناک می باشند ، در حقیقت این محصول می تواند برنامه های تهدید کننده نظیر ویروس ها را تشخیص دهد.

این محصول با استفاده از یک مدل امنیتی تعریف شده در تکنولوژی MPSتوانایی درک تهدیدات ناشناخته را دارا می باشد.

- **What is the MPS (Main Protection System)?**

MPS اساسا یک روشی است برای این که به شما نشان دهد چه برنامه هایی به واسطه سیستم عامل فعال شده و کدام به صورت غیر قانونی دارند به فعالیت خود ادامه می دهند.

این تکنولوژی را می توان به صورتی پیکربندی کرد که به صورت اتوماتیک بتواند تهدیدات نظیر ویروس را شناسایی و پاکسازی نماید.

این تکنولوژی می تواند تهدیداتی را که در پروسه ها (برنامه های کامپیوتری) ، داریورهای تحت هسته و درایورهای کاربری ، سرویس های ویندوز ، DLLهای ویندوز ، DLLهای غیر مجاز ،کلید های رجیستری و دسترسی برنامه ها به اینترنت را نمایش دهد. تمامی این موارد با استفاده از محدودی تراست قابل دسترسی است.

اگر شما برروی سیستم عامل خود برنامه هایی رانصب کرده اید باید آن را به وناک معرفی کنید تا به عنوان تهدید شناسایی نشوند.

از ثبت کردن پروسه های ناشناخته جدا خوداری کنید.

MPSچه تهدیداتی را می تواند شناسایی کند

شما در لیست زیر تهدیدات و تکنیک هایی را که وناک و MPSمی توانند شناسایی کنند را می بینید:

- ✓ یک ویروس که به واسطه ابزارهای جانبی نظیر لوازم ملتی مدیا یا درایو های سریال USB به سیستم شما حمله کرده اند.
- ✓ یک ورم یا ویروس که به واسطه ایرادات نرم افزاری که در سیستم شما بوده است می خواهد به شما آسیب برساند.
- ✓ یک ورم یا ویروس که بخواهد خود را به نحوی مخفی کند یا کاربر و یا سیستم عامل را فریب دهد.
- ✓ انواع روتکیت های نصب شده بر روی سیستم شما شامل تکنیک های
  - روتکیت های تحت هسته
  - روتکیت های تحت کاربر
- ✓ درایورهای نصب شده توسط برنامه ها و نام و مشخصات آن ها .
- ✓ سرویس های مجاز و نحوی فعالیت و همچنین علت آن ها .
- ✓ شناسایی اکثر برنامه های هکری مانند Backdoorsو اکسپولیت های ویندوزی.
- ✓ پروسه ها و درایور های مخفی در سطح سیستم عامل (تمامی سیستم عامل ها پشتیبانی می شوند)
- ✓ برنامه های که قصد دارند به نحوی خود را به اجرای مجدد برسانند.
- ✓ فایل هایی اجرایی که در نقاط حساس سیستم شما هستند و امضا آنها یکسان می باشد.
- ✓ DLLهایی که به صورت غیر مجاز به سیستم و برنامه های کاربردی دیگر آسیب می رسانند.

MPS Capabilities

MPSیا Main Protection Systemدارای یک زمان سنج می باشد که با استفاده از این زمان سنج می تواند به صورت دوره ای تست هایی را برای تشخیص ابزارهای ناشناخته (ویروس ها) و پاکسازی آن ها اقدام کند.

چنانچه MPSتشخیص دهد که یک پروسه جدید شروع به فعالیت کرده است در صورتی که پروسه ناشناس باشد به صورت خودکار و خارج از سیستم زمان بندی خود شروع به گرفتن تست از سیستم شما می کند.

MPSسعی دارد به شما نشان دهد که کدام برنامه یا پروسه ای می توانند یک ویروس باشند ، این ابزار علت هایی را که به واسطه آن می توان پروسه مشکوک را تشخیص دهید را نیز برای شما به لیستی اضافه می کند.

همچنین با استفاده از رنگ بندی پروسه ها سعی در نمایش وضعیت تهدید کنندگی آن ها دارد.

این ابزار همواره سرویس ها ، داریورها ، و کلید های رجیستری استارت آپ را به شما نشان می دهد تا شما نسبت به اجرای آن ها آگاهی پیدا می کنید.

- MPS Test Checks
    - If you want know more about MPS test Checks please see following link

      http://www.u0vd.org/Docs/White_Paper.pdf

Support Viruses and Rootkits techniques

For more information about techniques Please see

- www.Rootkit.com

- DKOM (Direct kernel Object Manipulation)

  This new technique is called direct kernel-object manipulation or DKOM.

  DKOM enables kernel mode Rootkits to modify kernel structures that exist in Memory such as lists of active processes and loaded drivers.

- Hook Processes MDL (Memory Descriptor List)
- TCP IRP (I/O Request Packet) Hook
- Hiding Processes by Doctoring the PspCidTable
- BASIC ROOTKIT
- The other Hiding Processes using an SSDT Hook
- Hooking modules (Inline , Detour)
- Hooking Services and Drivers

None support things

- SYSENTER 2E
- Privileged hooks
- NTFS Streams
- Hooking Interrupt Descriptor Table (IDT)

VA's New Technologies

New Technologies / Methods	MPS Support	Manually Checks	Validity Scanning
Processes/Modules	Yes	Yes	Yes
Device Drivers	Yes	Yes	Yes
Services	Yes	Yes	Yes
Kernel Drivers	Yes	Yes	Yes
Hooking Modules	Yes (Not All)	Yes	Yes
FPL (Fast Process List)	No	Yes	No
IAT	No	Yes	No
Threat Files	No	Yes	No
Freeze	Yes	Yes	No
Startup Files	Yes	Yes	Yes
Process Tree	No	Yes	No
SSDT	Yes	Yes (Not All)	No
Sensitive Threat	Yes	Yes	Yes
GUI Scanning	Yes	No	Yes
Parent PID Validity	Yes	Yes	Yes
GDI Scanning	Yes	No	Yes
EProcess Problem	Yes	Yes	Yes
DLL Information	Yes	No	Yes
Hidden File	No	Yes	No
Same Executable Folder	Yes	No	Yes
Files Scanning	Yes(not Automatic)	Yes	No
Process Call other Executable File	Yes	No	Yes
ICMP packets	Yes	Yes	No
MD5 signatures	Yes(not Automatic)	Yes	No
Binders Detection	Yes(not Automatic)	Yes	No
DKOM	Yes	Yes	Yes
Hook MDL	Yes	Yes	Yes
TCP/UDP IRP Hooks	No	Yes	Yes
Some SSDT Hook	Yes (Not All)	Yes (Not All)	No
Hooking modules	Yes (Not All)	Yes	Yes
SYSENTER 2E	Not Yet	Not Yet	Not Yet

Privileged hooks	Not Yet	Not Yet	Not Yet
NTFS Streams	Not Yet	Not Yet	Not Yet
Hooking IDT	Not Yet	Not Yet	Not Yet
Signature Checks	No	Yes	No

Help

- **U0vd Website (Support and Update)**

  http://www.u0vd.org

- **Contact us**

  Support Team

  Support AT u0vd.org

  Any Information about VA

  Info AT u0vd.org

  Contact with Manager of u0vd security

  Nima AT u0vd.org