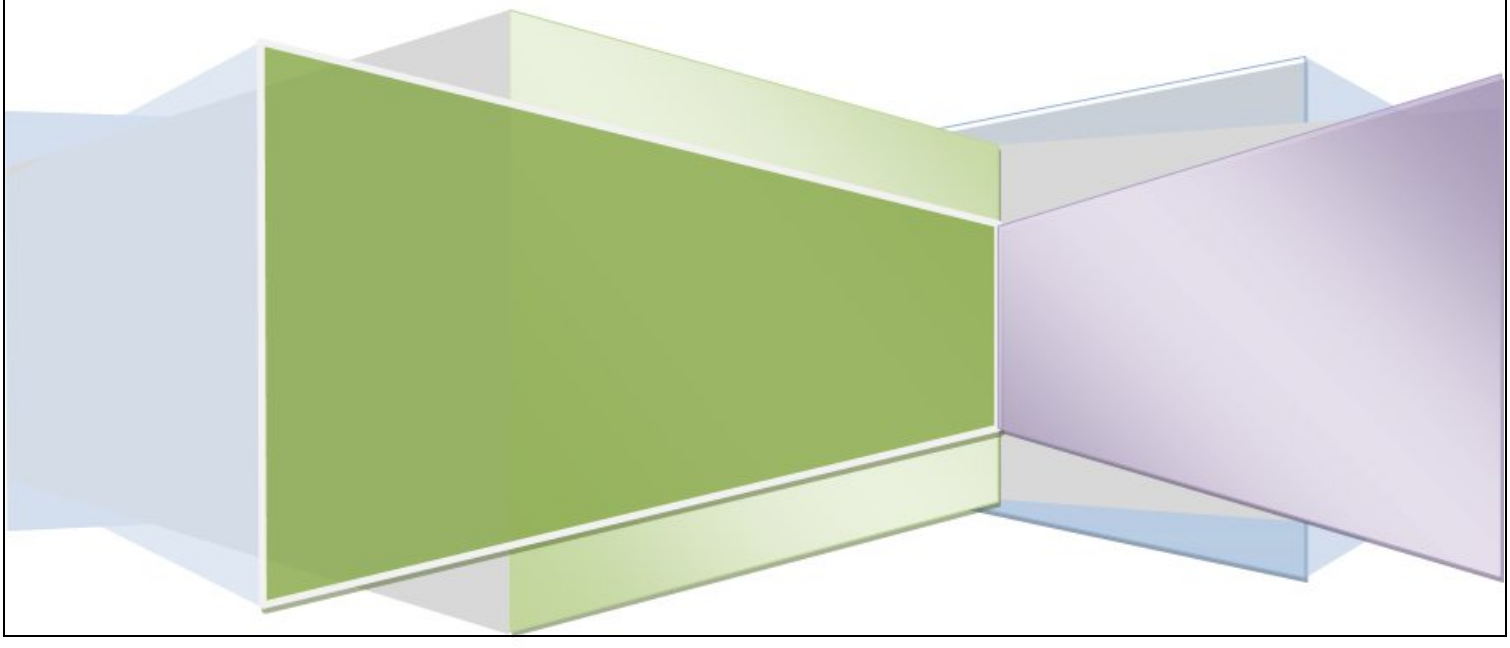
بسم الله الرحمن الرحیم

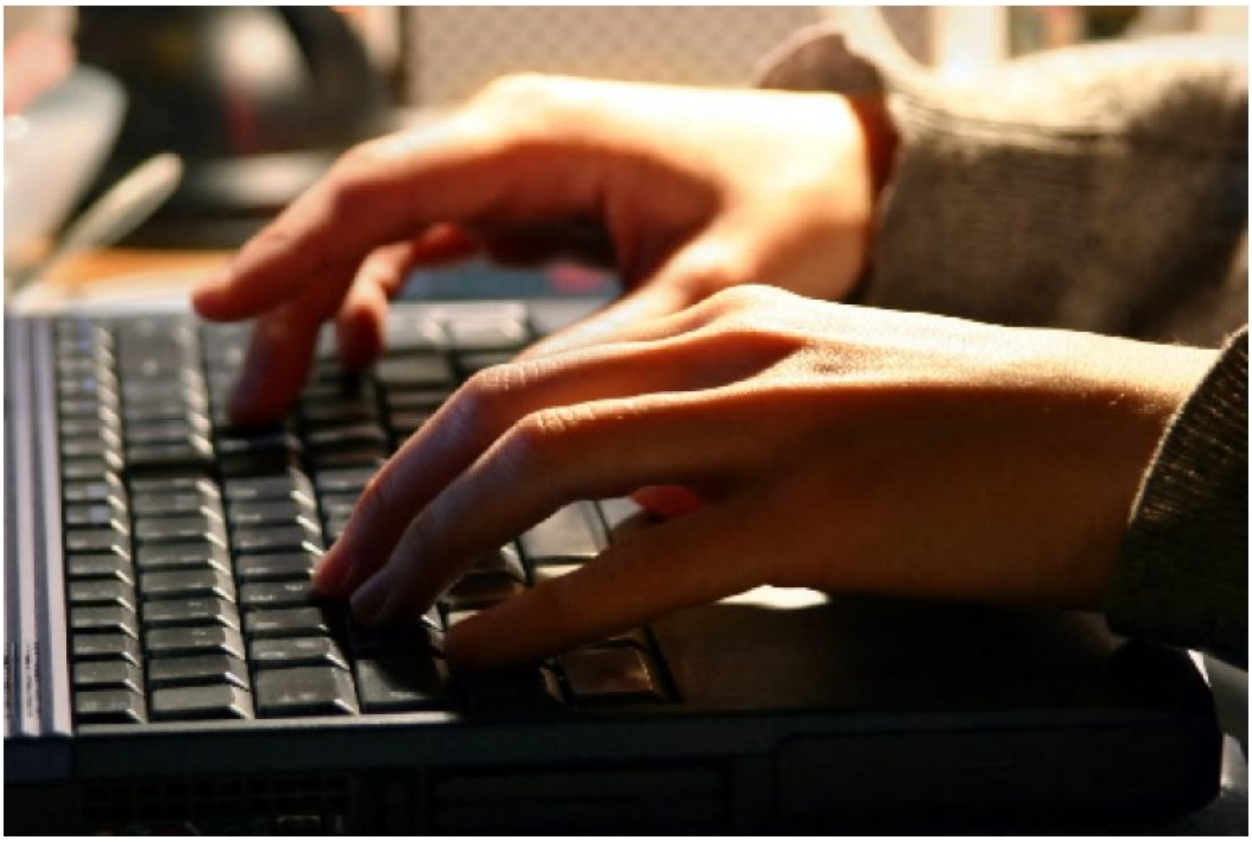
روت کیت چیست؟

نویسنده:عادل رحیمی

ایمیل:Rahimi.adel@Gmail.com



فهرست:



3

مقدمه ای بر روت کیت ها:

روت کیت[1]ها برنامه هایی هستند که از نظر کاربرد و ساختاری بسیار شبیه به تروجان[2] ها و بکدور[3] ها هستند با این تفاوت که شناختن و از بین بردن روت کیت ها بسیار مشکل تر از بکدور ها و تروجان هاست زیرا تروجان ها فقط با اضافه کردن فایلی به کامپیوتر اجرا میشوند اما روت کیت ها جایگزین بعضی برنامه های ویندوز یا گاهی جایگزین کرنل[4] میشوند ! و به هکر اجازه میدهند که از روت کیت به عنوان یک بکدور و یا شنونده[5] استفاده کند و در آخر هکر میتواند با نصب یک اسنیفر[6] در عمق سیستم قربانی به راحتی اطلاعاتی که نیاز دارد را بدست آورد.

انواع روت کیت ها:

روت کیت ها پنج نوع اند که در ادامه هریک رو به اختصار توضیح میدهیم.

Firmware, hypervisor, kernel, library and application

تعریف انواع روت کیت ها:

- Hardware/Firmware level

Firmware در لغت به معنی نرم افزاری دائمی است یعنی نرم افزاری که در حافظه فقط خواندنی ROM[7] قرار داده شده است و این نوع روت کیت ها نیز معمولا خود را در Firmware مخفی میکنند لازمه بگم که این نوع روت کیت ها از خطرناک ترین نوع روت کیت ها هستند.

---

[1] Rootkit or Root kit
[2] Trojan
[3] Backdoors
[4] Kernel
[5] Listener
[6] Sniffer
[7] Read only memory

در اکتبر 2009 محققان نوعی روت کیت سطح BIOS رو برای کامپیوتر های خانگی گزارش دادند که میتواند تمام هارد دیسک رو از بین ببرد و حتی توانایی نصب کردن دوباره ی سیستم عامل را هم دارد!!

- Hypervisor level

این روت کیت ها با دستکاری کردن در مراحل بوت شدن سیستم خود را در سیستم عامل اصلی به صورت یک مدیر[1] جا میزنند!

حتی این نوع روت کیت ها میتواند سیستم عامل اصلی رو به صورت یک سیستم عامل مجازی بارگزاری کند

از این خانواده میتوان Blue pill و SubVirt را نام برد که SubVirt یکی از روت کیت های آزمایشگاهی است که توسط شرکت مایکروسافت و دانشگاه Michigan توسعه داده میشود (در حال حاضر اطلاعاتی در مورد Blue pill در اختیار ندارم).

- Kernel level

این روت کیت ها کد(ی/هایی) را به هسته اضافه یا جایگزین میکنند که باز هم به هکر اجازه ی دسترسی به سیستم در حد مدیر[2] میدهد.

اولین روت کیت از این خانواده نیز در دهه ی 1990 توسط Greg Hoglund برای Windows NT 4.0 نوشته شد که در مورد این روت کیت هم اطلاعات زیادی ندارم.

[1] Hypervisor
[2] Root / Administrator / Super user

- Library Level

این نوع روت کیت ها معمولا با تغییر/جابجایی سیستم کال[1] با نسخه ای که اطلاعات هکر رو مخفی کند کار میکنند.

- Application Level

این روت کیت ها تنها با دستکاریِ برنامه ها یا تزریق کدی در آنها رفتار برنامه را تغییر یا به کلی آن را در دست میگیرند!

نحوه ی مقابله با روت کیت ها:

مهمترین راه مقابله با روت کیت ها اجازه ندادن به هکر در دسترسی به حساب مدیر است اگر ما بتوانیم تمام راه های نفوذ و آسیب های جدیدِ سیستم عاملمان را شناسایی و آن ها را از بین ببریم شانس دستیابی هکر به حساب ریشه[2] ی سیستم خود را تقریبا به صفر رسانده ایم.

نحوه ی شناسایی روت کیت ها:

- استفاده از برنامه ی ChRootkit این برنامه به صورت خودکار تمام دایرکتوری ها رو از قبیل:

/bin/login چک میکند تا از وجود روت کیت با خبر شود.

[1] System call - The mechanism used by an application program to request service from the operating system. System calls often use a special machine code instruction which causes the processor to change mode (e.g. to "supervisor mode" or "protected mode"). This allows the OS to perform restricted actions such as accessing hardware devices or the memory management unit.
[2] Root

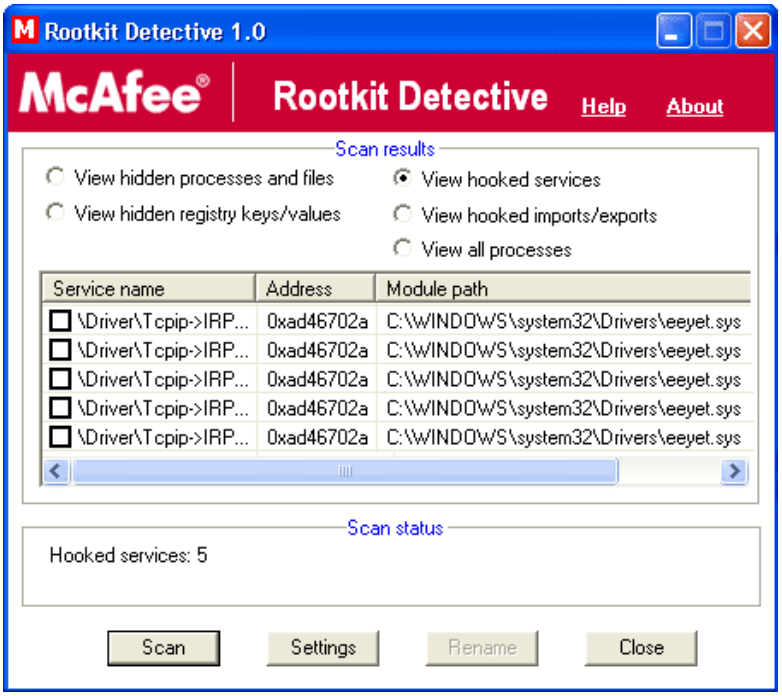
- TripWire ابزاری است که درهم سازیِ MD5 ای از فایل های بحرانی مانند: etc/passwd/bin/login ساخته و به صورت دوره ای آن را با پایگاه داده ای امنی مقایسه میکند در صورت تغییر در MD5یک سرویس سریع به مدیر اطلاع میدهد.

نحوه ی پاکسازی روت کیت ها:

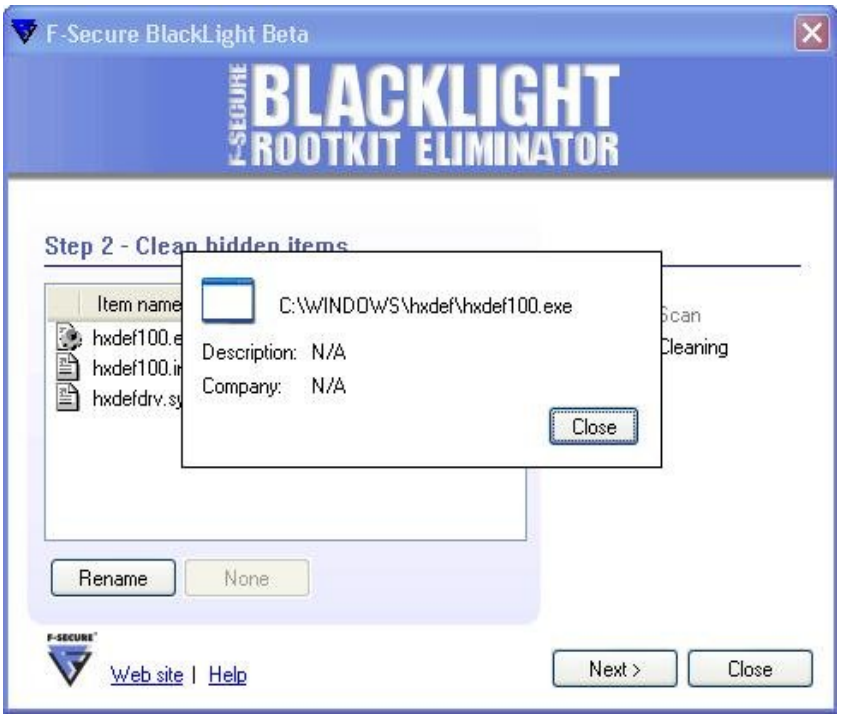
استفاده از ابزار هایی مانند:

- Sophos Anti-Rootkit

McAfee Rootkit Detective ●



F-Secure Blacklight ●



در بین این نرم افزارها فقط Sophos Anti-Rootkit رایگان است

8 منابع:

منابع انگلیسی:

- Brumley, David (1999-11-16). "invisible intruders: rootkits in practice". USENIX. http://www.usenix.org/publications/login/1999/features/rootkits.html.
- Mark Russinovich (2005-10-31). "Sony, Rootkits and Digital Rights Management Gone Too Far". http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx. Retrieved on 2008-09-15.
- "New backdoor program uses Sony rootkit". Kaspersky Lab. 2005-11-10. http://www.kaspersky.com/news?id=173733204. Retrieved on 2008-09-15.
- "Sony's long-term rootkit CD woes". BBC News. 2005-11-21. http://news.bbc.co.uk/2/hi/technology/4456970.stm Retrieved on 2008-09-15.
- Russinovich, Mark (2006-02-06). "Using Rootkits to Defeat Digital Rights Management". *Winternals*. SysInternals. Archived from Using Rootkits to Defeat Digital Rights Management the original on 2006-08-31. http://blogs.technet.com/markrussinovich/archive/2006/02/06/using-rootkits-to-defeat-digital-rights-management.aspx. Retrieved on 2006-08-13.
- Mark Russinovich (June 2005). "Unearthing Root Kits". Windows IT Pro. http://www.windowsitpro.com/Article/ArticleID/46266/46266.html.
- Implementing and Detecting an ACPI Rootkit by John Heasman, presented at BlackHat Federal, 2006.
- Implementing and Detecting a PCI Rootkit by John Heasman, November 15, 2006.
- Austin Modine (2008-10-10). "Organized crime tampers with European card swipe devices: Customer data beamed overseas". The Register. http://www.theregister.co.uk/2008/10/10/organized_crime_doctors_chip_and_pin_machines/. Retrieved on 2008-10-13.
- Dan Goodin (2009-03-24). "Newfangled rootkits survive hard disk wiping". The Register. http://www.theregister.co.uk/2009/03/24/persistent_bios_rootkits/ Retrieved on 2009-03-25.
- "SubVirt: Implementing malware with virtual machines" (PDF). University of Michigan, Microsoft. 2006-04-03. http://www.eecs.umich.edu/virtual/papers/king06.pdf Retrieved on 2008-09-15.
- The 64-bit version of Windows XP and Server 2008 are a notable exception "Driver Signing Requirements for Windows". Microsoft. http://www.microsoft.com/whdc/winlogo/drvsign/drvsign.mspx. Retrieved on 2008-07-06.
- Rootkit Evolution by Alisa Shevchenko (1 September 2008), An Overview of Unix Rootkits by Anton Chuvakin (February 2003)
- "Signing and Checking Code with Authenticode". Microsoft. http://msdn.microsoft.com/en-us/library/ms537364(VS.85).aspx. Retrieved on 2008-09-15.

- "RootkitRevealer v1.71". Microso Technet. 200611-01. http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx. Retrieved on 2008-10-10.
- "Stopping Rootkits at the Network Edge" (PDF). Trusted Computing Group. 2007-01-04. h ps://www.trustedcompu nggroup.org/news/Industry Data/Whitepaper Rootkit Strom v3.pdf. Retrieved on 2008-07-11.
- "Rootkit Question". Spywareinfoforum.com. h p://www.spywareinfoforum.com/lofiversion/index.php/t52360.html. Retrieved on 2009-04-07.
- Posted by Flashlight (2007-04-30). "Tech Loop: Rootkits: The next big enterprise threat?". Techloop.blogspot.com. h p://techloop.blogspot.com/2007/04/rootkits-next-big-enterprise-threat.html. Retrieved on 2009-04-07.
- "Security Watch: Rootkits for fun and profit - CNET Reviews". Reviews.cnet.com. 2007-01-19. h p://reviews.cnet.com/4520-3513_7-6686763-1.html. Retrieved on 2009-04-07.
- Sponsored by Dell. "Six ways to fight back against botnets - Business Center". PC World. h p://www.pcworld.com/businesscenter/ar cle/137821/six_ways_to_fight_back_against_botnets.html. Retrieved on 2009-04-07.
- 12:00 AM. "Handling Today's Tough Security Threats: Rootkits - Malicious Code - STN Peer-to-Peer Discussion Forums". Forums.symantec.com. h ps://forums.symantec.com/t5/Malicious-Code/Handling-Today-s-Tough-Security-Threats-Rootkits/ba-p/305215;jsessionid=7D537BC23D36E015CD11EA806B389E54#A68. Retrieved on 2009-04-07.
- Hultquist, Steve (2007-04-30). "Rootkits: The next big enterprise threat? | Security Central". InfoWorld. h p://www.infoworld.com/ar cle/07/04/30/18FErootkit_3.html. Retrieved on 2009-04-07.

منبع فارسی:

"مقاله ی روت کیت چیست؟" از شرکت امنیتی آشیانه

لازم به ذکر است که این **اولین** مقاله یِ تخصّصی در رابطه با روت کیت ها به زبان فارسی است .