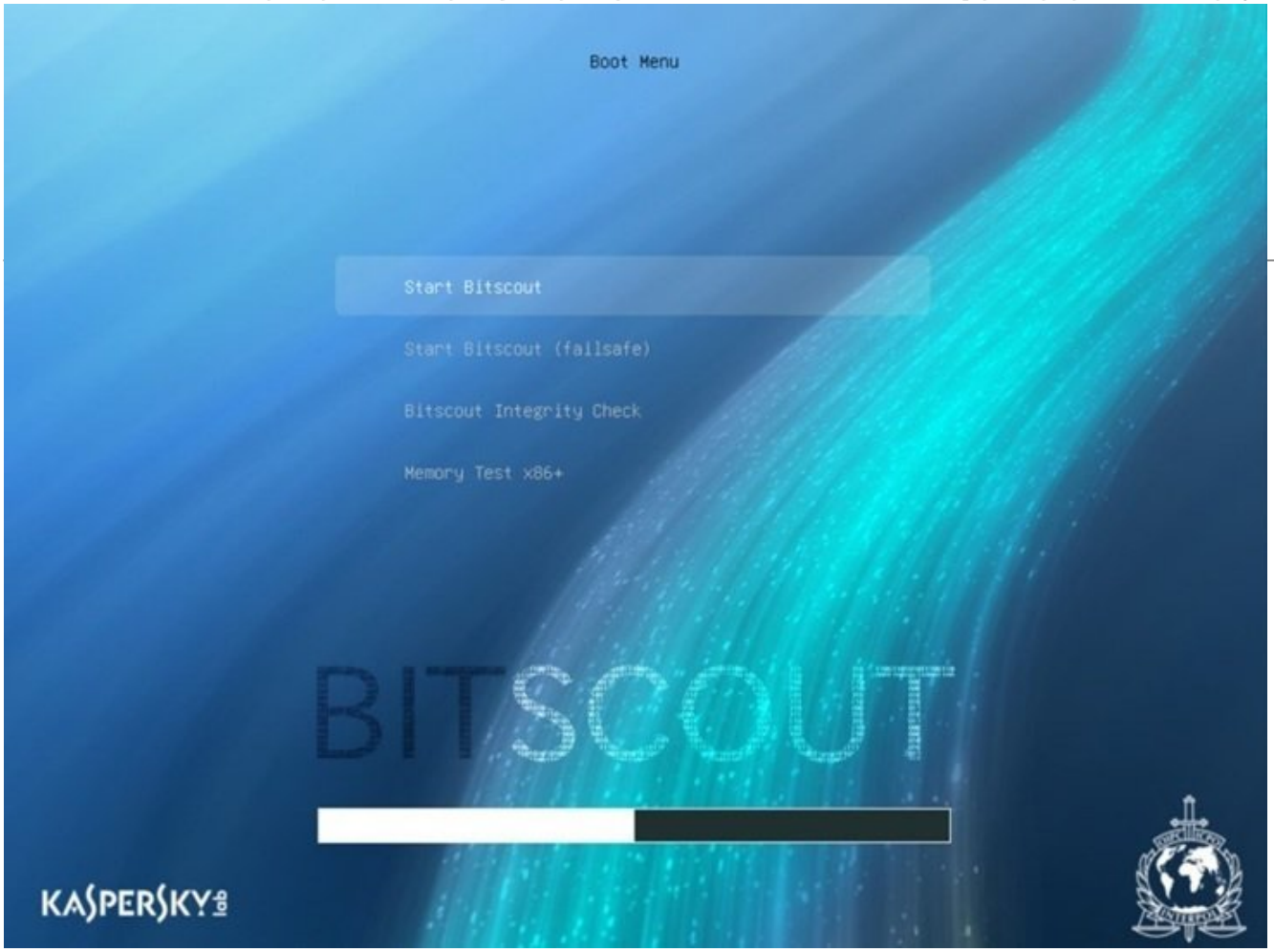
جرم‌شناسی دیجیتالی از راه دور

کسپرسکی ابزار جرم‌شناسی دیجیتالی متن‌باز خود را منتشر کرد



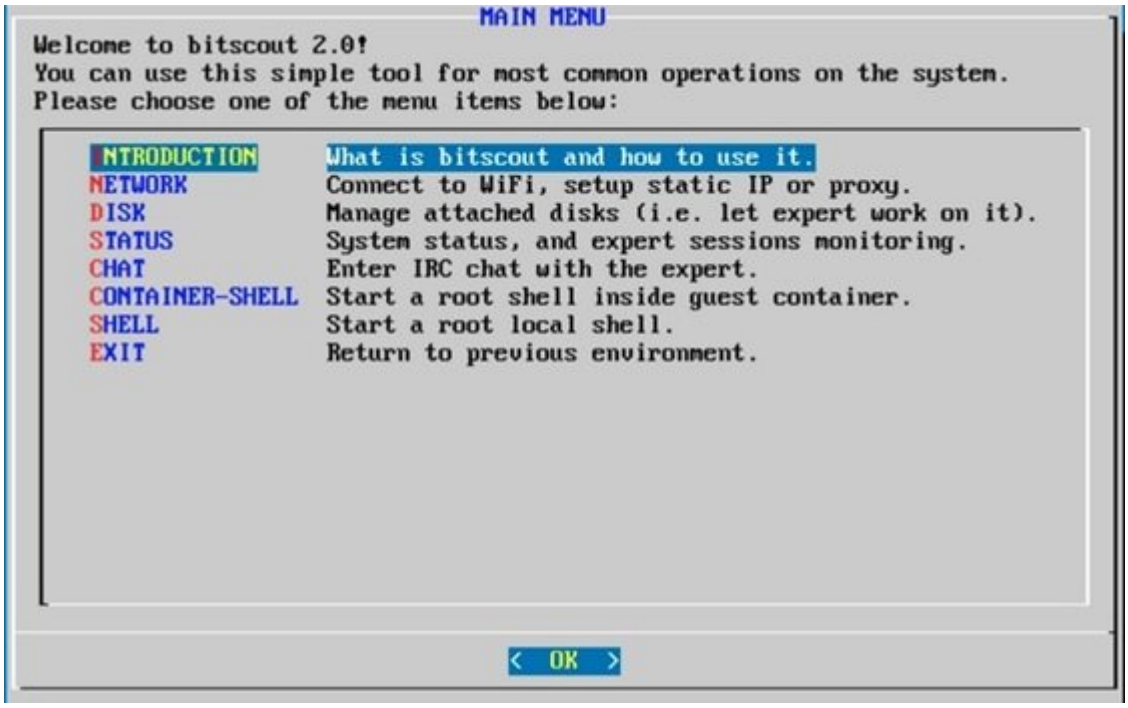
ویتالی کاملوک یکی از پژوهشگران امنیتی آزمایشگاه کسپرسکی به تازگی ابزار متن بازی موسوم به Bitscout را منتشر کرده است. Bitscout یک ابزار بهینه و کاملا ایده‌آل است که در زمینه جرم‌شناسایی دیجیتالی از راه دور می‌تواند مورد استفاده قرار می‌گیرد.

در حالی که ابزار فوق جزء یکی از محصولات رسمی شرکت کسپرسکی به شمار نمی‌رود، اما فرآیند ساخت و توسعه آن از چند سال قبل آغاز شده و به مرور زمان بر اساس نیازهای این شرکت در زمینه جرم‌شناسی دیجیتالی بهبود پیدا کرده است. در شرایطی که نسخه 1 این محصول هیچ‌گاه به‌طور عمومی منتشر نشد، اما نسخه دوم این محصول که اکنون به صورت عمومی منتشر شده است به کارشناسان حوزه امنیت این توانایی را می‌دهد تا از راه دور به تجزیه و تحلیل یک سامانه بپردازند.

مطلب پیشنهادی

دفاع همه جانبه در برابر هکرها
مایکروسافت ویندوز 10 را به ابزار ضد باج‌افزاری دیگری تجهیز می‌کند

این بررسی در شرایطی انجام می‌شود که مالک سیستم بر عملیات فوق نظارت داشته و اطمینان حاصل می‌کند که این دسترسی‌های کارشناسانه تنها به دیسک‌های هدفی که مشخص کرده است محدود می‌شوند. این ابزار برای پژوهشگران امنیتی، واحدهای بررسی جرایم سایبری و همچنین نهادهای آموزشی یک ابزار ارزشمند به شمار می‌رود.



مالک دستگاه که در نظر دارد یک فرآیند تجزیه و تحلیل قانونی روی سامانه او انجام شود یک فایل ایمیج دریافت می‌کند که باید این فایل را روی یک رسانه ذخیره‌ساز قابل حمل رایت کند. در ادامه سامانه از طریق این درایو راه‌اندازی شده و پژوهشگر قادر است به ابزار Bitscout با استفاده از پروتکل SSH و از طریق VPN متصل شود. در حالی که ابزار فوق مشتمل بر یکسری ابزارهای مفید و محبوب در زمینه تجزیه و تحلیل قانونی و جرم‌شناسی است، اما کاربران این توانایی را دارند تا ابزارهای فوق را سفارشی‌سازی کرده یا ابزارهای موردنظر خود را به آن اضافه کنند. این ابزار همچنین مجهز به یک رابط کاربری متنی تجهیز شده تا کاربران به شکل ساده‌تری بتوانند از آن استفاده کنند.

مطلب پیشنهادی

بدافزاری که تنها اطلاعات سرقت می‌کند
تروجان SpyDleaer می‌تواند از 40 برنامه اندرویدی جاسوسی کند

کاملوک در این ارتباط گفته است: «محقق از طریق یک کانتینر مجازی که درون این ابزار قرار دارد، تنها مجوزهای دسترسی به دیسک‌هایی را در اختیار دارد که مالک دستگاه برای او مشخص کرده است. این رویکرد به منظور ممانعت از دسترسی‌های غیر مجاز به کار گرفته شده است. پژوهشگران این توانایی را دارند تا نرم‌افزارهای جانبی مورد نیاز خود را روی کانتینر نصب کرده و تغییرات مورد نیاز خود را اعمال کنند. در نتیجه پس از خاموش شدن سیستم همه چیز به حالت اولیه تغییر پیدا کرده و مشکل خاصی به وجود نمی‌آید. همه نشست‌های راه دور ضبط شده و خارج از کانتینر ذخیره‌سازی می‌شوند. در نتیجه سطح خوبی از ایزوله‌سازی به منظور بازسازی پرونده‌ها برای اهداف یادگیری یا ثبت شواهد به شکل معتبری انجام می‌شود.» کد متن باز این ابزار به همراه دستورالعمل‌های لازم برای استفاده از این ابزار در آدرس گیت‌هاب به نشانی bitscout قرار دارد.

تاریخ انتشار:

22 تیر 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/8690/%DA%A9%D8%B3%D9%BE%D8%B1%D8%B3%DA%A9%DB%8C-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1-%D8%AC%D8%B1%D9%85%E2%80%8C%D8%B4%D9%86%D8%A7%D8%B3%DB%8C-%D8%AF%DB%8C%D8%AC%DB%8C%D8%AA%D8%A7%D9%84%DB%8C-%D9%85%D8%AA%D9%86%E2%80%8C%D8%A8%D8%A7%D8%B2-%D8%AE%D9%88%D8%AF-%D8%B1%D8%A7-%D9%85%D9%86%D8%AA%D8%B4%D8%B1-%DA%A9%D8%B1%D8%AF