นักวิจัยแคสเปอร์สกี้ แลป คิดค้นซอฟต์แวร์ทูล “BitScout”

เพื่อจะได้ไม่ต้องเดินทางไปไกลๆ ที่โน่นที่นี่เพื่อเก็บรวบรวมหลักฐานจากคอมพิวเตอร์ที่โดนจู่โจมตกเป็นเหยื่อของอาชญากรรมไซเบอร์ ผู้เชี่ยวชาญของแคสเปอร์สกี้ แลปได้พัฒนาทูลอย่างง่ายที่สามารถเก็บรวบรวมข้อมูลสำคัญได้จากระยะไกลโดยไม่ต้องเสี่ยงต่อการกระจายแพร่เชื้อหรือการสูญหายของข้อมูล ทูลนี้ เรียกว่า BitScout (บิตสเก๊าต์) ทูลที่เป็นเสมือนมีดอันคมกริบในการสืบสวนหาหลักฐานจากระยะไกลจากระบบที่ยังทำงานอยู่ (live systems) และนักสืบสวนสามารถใช้ได้โดยไม่มีค่าใช้จ่าย

ในการจู่โจมโจมตีทางไซเบอร์ส่วนมาก เจ้าของที่ถูกต้องตามกฎหมายของระบบที่ถูกโจมตีจากผู้บุกรุกนิรนามนั้นมักจะยินยอมให้ความร่วมมือ และให้ความช่วยเหลือแก่นักวิจัยด้านความปลอดภัยในการค้นหาเวคเตอร์ที่ก่อให้เกิดการติดเชื้อ หรือรายละเอียดอื่นๆ ที่เกี่ยวข้องกับผู้บุกรุก อย่างไรก็ตาม ก็ยังเป็นความวิตกกังวลมาแสนนานของเหล่านักวิจัยด้านการพิสูจน์หลักฐานถึงความจำเป็นที่จะต้องเดินทางไกลเพื่อเก็บรวบรวมหลักฐานเบาะแสสำคัญ อาทิ ตัวอย่างมัลแวร์จากคอมพิวเตอร์ที่ติดเชื้อ ซึ่งนั่นย่อมหมายถึงค่าใช้จ่ายสูงและความล่าช้า ยิ่งยืดเยื้อในการทำความเข้าใจลักษณะการจู่โจมนั้น การป้องกันผู้ใช้งาน และชี้ตัวผู้ทำการบุกรุกก็จะยิ่งเนิ่นนานออกไป ส่วนทางเลือกอื่นๆ ก็จะต้องอาศัยเครื่องมือที่มีราคาแพง รวมทั้งความรู้ในการใช้งานทูลเหล่านั้น หรือเสี่ยงติดเชื้อมัลแวร์ไปด้วย หรือหลักฐานสูญหายระหว่างการย้ายข้อมูลระหว่างเครื่องคอมพิวเตอร์

เพื่อเป็นการแก้ปัญหานี้ วิตาลี คามลัก ผู้อำนวยการทีมวิเคราะห์และวิจัย (Global Research and Analysis Team หรือทีม GReAT) แคสเปอร์สกี้ แลป ประจำภูมิภาคเอเชียแปซิฟิก จึงได้คิดค้นเครื่องมือดิจิทัลที่เป็นโอเพ่นซอร์สขึ้น สามารถใช้งานในระยะไกลเพื่อทำการเก็บรวบรวมหลักฐานสำคัญ เก็บรวบรวมภาพรวมของดิสก์ผ่านระบบเครือข่าย หรือเก็บลงบนสตอเรจที่ต่อเชื่อมอยู่ หรือเพียงแต่จะให้ความช่วยเหลือในการจัดการกับมัลแวร์ก็ย่อมได้ สามารถเรียกดูได้และทำการวิเคราะห์ข้อมูลที่เกี่ยวโยงกับหลักฐานได้จากระยะไกล หรือจะวิเคราะห์ ณ ที่เกิดเหตุก็ได้ โดยที่สตอเรจจัดเก็บข้อมูลหลักนั้นยังคงใช้การได้อยู่ โดยแยกใช้งานผ่านที่เก็บข้อมูลที่แยกต่างหากที่สามารถไว้วางใจเชื่อถือได้

“ความต้องการที่จะวิเคราะห์เหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความปลอดภัยให้ได้ผลดีและรวดเร็วเท่าที่จะเป็นไปได้นั้นได้กลายมาเป็นประเด็นที่มีความสำคัญอย่างยิ่ง เนื่องจากฝ่ายตรงข้ามหรือผู้ร้ายได้เติบโตแข็งแกร่งก้าวหน้าตามจับตัวยากขึ้นทุกที แต่ความเร็วที่ไม่เกี่ยงราคาค่าใช้จ่ายนั้นก็ไม่เป็นที่พึงประสงค์เช่นกัน – เราจำเป็นต้องทำให้แน่ใจว่าหลักฐานที่เก็บได้นั้นต้องไม่ด่างพร้อย ถูกต้องเพื่อที่กระบวนการสืบสวนนั้นได้รับความไว้วางใจ และผลลัพธ์ที่ได้

รับมีคุณภาพความแม่นยำสำหรับใช้เป็นหลักฐานในศาลยุติธรรมได้หากมีความจำเป็นต้องใช้ ผมไม่พบเครื่องมือใดที่สามารถทำให้เราได้ทุกอย่างตามที่ต้องการเหล่านั้น และไม่มีความยุ่งยากซับซ้อน – ดังนั้น ผมจึงตัดสินใจคิดค้นสร้างขึ้นมาเอง” วิตาลี กล่าว

ผู้เชี่ยวชาญแคสเปอร์สกี้ แลปทำงานอย่างใกล้ชิดกับหน่วยงานบังคับใช้กฎหมายทั่วโลกเพื่อให้ความช่วยเหลือในการวิเคราะห์เชิงเทคนิคในการทำการสืบสวนทางไซเบอร์ ซึ่งจะทำให้ได้รับข้อมูลเชิงลึกที่มีความเฉพาะตัวเกี่ยวโยงกับความท้าทายที่ทางเจ้าหน้าที่บังคับใช้กฎหมาย (LEA personnel) ต้องเผชิญในยามที่ต่อสู้กับอาชกรรมไซเบอร์สมัยใหม่ รูปแบบระบบความปลอดภัยทางไซเบอร์ในปัจจุบันนี้มีความซับซ้อน และก้าวหน้ามากจนกระทั่งเจ้าหน้าที่ต้องอาศัยเครื่องมือที่สามารถปรับตัวรองรับการใช้งาน และปรับตามขนาดให้เข้ากับความจำเป็นในการใช้งานแต่ละกรณีได้ โดย BitScout นี้ถือเป็นตัวอย่างที่ดี สามารถปรับให้ตรงตามที่เจ้าหน้าที่สืบสวนต้องการ และปรับปรุง อัพเกรดด้วยฟีเจอร์ที่เพิ่มเข้ามา รวมทั้งซอฟต์แวร์ที่สร้างตามคำสั่งเฉพาะ สิ่งที่สำคัญที่สุด คือ เครื่องมือนี้ไม่มีค่าใช้จ่าย สร้างบนโอเพ่นซอร์สโซลูชั่น และโปร่งใสเข้าใจง่าย แทนที่จะต้องพึ่งพาอาศัยเครื่องมือจากเธิร์ดปาร์ตี้ที่ใช้โค้ดเฉพาะค่ายของตนเองเท่านั้น ผู้เชี่ยวชาญสามารถใช้โอเพ่นซอร์สโค้ดของ Bitscout เพื่อสร้างเครื่องมืออันเฉียบคมสำหรับใช้ในการพิสูจน์หลักฐานดิจิทัลเป็นของตนเองได้

รายการฟีเจอร์ของ BitScout ประกอบด้วย

- การเก็บภาพรวมของดิสก์ (Disk image acquisition) ที่แม้แต่พนักงานที่ไม่เคยผ่านการอบรมก็สามารถทำเองได้
- ฝึกอบรมระหว่างดำเนินการใช้งาน (แชร์ภาพเซสชั่นของเครื่องคอมพิวเตอร์ให้ดูได้)
- โอนย้ายข้อมูลที่มีความซับซ้อนไปยังห้องปฏิบัติการของคุณเพื่อการตรวจสอบเชิงลึก
- ใช้วิธีการตรวจสอบแบบ Yara หรือ ทำการสแกน AV ระบบช่วงที่ออฟไลน์ได้จากระยะไกล (สำคัญสำหรับการตรวจสอบรูทคิท)
- ค้นหาและเรียกดูคีย์ลงทะเบียน (registry keys) (autoruns, บริการ, อุปกรณ์ยูเอสบีที่เชื่อมต่ออยู่)
- ดำเนินการกู้คืนไฟล์ที่ถูกลบออกไปแล้วได้จากระยะไกล
- ฟื้นฟูปรับปรุงสถานะระบบระยะไกล หากได้รับสิทธิ์ในการเข้าใช้ระบบจากผู้เป็นเจ้าของระบบ
- ทำการสแกนโหนดบนเครือข่ายอื่นๆ ได้จากระยะไกล (เป็นประโยชน์สำหรับการรับมือกับเหตุการณ์จากระยะไกล)

เครื่องมือนี้มีพร้อมให้ใช้งานได้โดยไม่มีค่าใช้จ่ายที่ศูนย์เก็บโค้ด GitHub:
https://github.com/vitaly-kamluk/bitscout
สามารถอ่านข้อมูลเพิ่มเติมได้จาก
http://securelist.com/bitscout-the-free-remote-digital-forensics-tool-builder/78991/