แคสเปอร์สกี้ แลป เผย มัลแวร์ภัยไซเบอร์ตัวร้ายบางตัวต้นทุนต่ำแต่มีอันตรายร้ายแรงต่อองค์กรธุรกิจ

นักวิจัยจากแคสเปอร์สกี้ แลปสังเกตว่าปัจจุบันภัยไซเบอร์มีความซับซ้อนในกลการปฏิบัติการโจมตีเพิ่มขึ้นอย่างมีนัยยะสำคัญ เป็นเรื่องที่รู้กันทั่วไปว่าผู้ร้ายไซเบอร์มักจะไม่ใช้เทคนิคโจมตีที่มีราคาแพงหรือซับซ้อนอย่าง ช่องโหว่ zero-day เท่าใดนัก แต่มักใช้วิธีการคุกคามผ่านแคมเปญสังคมออนไลน์ วิศวกรรมสังคม ในการรุกเข้าหาเหยื่อควบคู่ไปกับการใช้เทคนิคร้ายกาจต่างๆ ที่เป็นรู้จักกันอยู่ ผู้ร้ายไซเบอร์เหล่านี้จึงได้ผลลัพธ์สมดั่งใจ คือ แคมเปญร้ายที่บรรดาโซลูชั่นซีเคียวริตี้ที่ใช้กันตามองค์กรธุรกิจทั่วไปนั้นจะตรวจจับได้ยากมาก

การเปลี่ยนแปลงยกระดับวิธีปฏิบัติการเช่นนี้แสดงให้เห็นว่า โครงสร้างสารสนเทศพื้นฐานโดยทั่วไปของบริษัทองค์กรต่างๆ ทุกวันนี้ล้วนมีจุดอ่อนพอที่ผู้ร้ายไซเบอร์จะอาศัยทูลเซ็ตที่สนนราคาไม่เท่าไรก็สามารถบุกเจาะเข้าไปได้แล้ว อย่างเช่น Microcin ซึ่งเป็นแคมเปญร้ายที่ถูกตรวจจับได้โดยผู้เชี่ยวชาญของแคสเปอร์สกี้ แลปเมื่อเร็วๆ นี้ เป็นแคมเปญโจมตีที่ราคาถูกแต่มีอันตรายสูง

ทั้งหมดนี้เริ่มต้นเมื่อ Kaspersky Anti Targeted Attack Platform (KATA) ได้พบไฟล์ RTF ที่ดูน่าสงสัย มี exploit (มัลแวร์ที่อาศัยช่องโหว่ด้านความปลอดภัยตามซอฟท์แวร์ยอดนิยมเพื่อแอบติดตั้งคอมโพเน้นท์ไม่พึงประสงค์เข้าไป) ของช่องโหว่ในไมโครซอฟท์ออฟฟิศที่ได้รับการแก้ไขไปเรียบร้อ้ยแล้ว แต่ก็ไม่แปลกที่มิจฉาชีพไซเบอร์จะใช้ exploits ที่รู้กันดีอยู่แล้วเพื่อแพร่กระจายเข้าหาเหยื่อ เป็นช่องทางกระจายมัลแวร์สู่วงกว้าง แต่เมื่อศึกษาลงลึกกลับพบว่า ไฟล์ RTF นี้ไม่ได้เป็นของกลุ่มที่ระบาดอยู่ แต่กลับเป็นของแคมเปญ ที่ตั้งเป้าหมายที่เหยื่ออย่างชัดเจนและมีการทำงานที่ถือว่าซับซ้อนกว่ามาก ไฟล์เอกสารที่ทำหน้าที่เป็นสเปียร์ฟิชชิ่งจะถูกแพร่กระจายผ่านไซต์เฉพาะกลุ่ม เช่น ฟอรั่มเงินกู้ซื้อบ้าน เป็นต้น

เมื่อ exploit ถูกกระตุ้นให้ทำงาน มัลแวร์ที่มีโครงสร้างเป็นโมดูล (modular structure) จะถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของเหยื่อ โดยใช้วิธีการ injectionเข้ามาที่ไฟล์ iexplorer.exe และตัวออโต้รันในโมดูลนี้ก็จะทำงานผ่าน dll-hijacking ซึ่งเป็นเทคนิคที่เป็นที่รู้จักและใช้กันแพร่หลาย

ท้ายที่สุด เมื่อโมดูลหลักได้รับการติดตั้งแล้ว โมดูลเสริมบางโมดูลก็จะถูกดาวน์โหลดมาจากคอมมานด์และคอนโทรลเซิร์ฟเวอร์ และจะมีอย่างน้อยหนึ่งโมดูลในนั้นที่ใช้ steganography – เป็นวิธีการปกปิดข้อมูลที่ซ่อนอยู่ภายในไฟล์

ที่ดูก็ไม่น่าจะมีอันตรายอะไร เช่น ภาพ แต่ก็ยังถือเป็นเทคนิคอีกประเภทหนึ่ง ที่ใช้ในการโอนย้ายถ่ายข้อมูลแบบไม่ให้ถูกจับได้

เมื่อวางแพลตฟอร์มที่ประสงค์ร้ายไว้พร้อมแล้ว มัลแวร์จะทำการค้นหาไฟล์ที่มี extensions เช่น .doc, .ppt, .xls, .docx, .pptx, .xlsx, .pdf, .txt และ .rtf จากนั้นเข้ารหัสเก็บไว้ใน archive รอส่งต่อไปให้ผู้ก่อการ นอกจากจะใช้เทคนิคที่รู้กันอยู่แล้วควบคู่ไปกับเทคนิคใหม่ๆ รวมทั้งแบคดอร์ที่รู้กันอยู่แล้วไปด้วย ซึ่งได้เคยพบเห็นกันในการโจมตีก่อนหน้านี้ และยังพบว่ามีใช้ทูลที่มีความถูกต้องมาประกอบด้วย โดยเป็นทูลที่สร้างขึ้นมาสำหรับทดสอบการเจาะเข้าระบบ (penetration testing) ซึ่งโดยมากมักจะผ่านการตรวจจับของซีเคียวริตี้โซลูชั่นไปได้โดยไม่ชี้ว่าเป็นมัลแวร์

“แต่หากนำมาทำการศึกษาแยกส่วนแล้วจะพบว่าการโจมตีประเภทนี้ไม่มีความร้ายแรงนัก โดยวงการซีเคียวริตี้ได้บันทึกรายละเอียดข้อมูลเกือบทุกคอมโพเน้นท์ไว้เรียบร้อยแล้ว จึงตรวจจับค่อนข้างง่าย อย่างไรก็ตาม ดูประหนึ่งว่ามัลแวร์พวกนี้จะมารวมตัวกันเพื่อก่อให้เกิดความยุ่งยากซับซ้อนกว่าเดิมกว่าที่จะตรวจพบการคุกคามได้ ที่สำคัญไปกว่านั้น แคมเปญแบบนี้ไม่ใช่มีอยู่เพียงหนึ่งเดียว เป็นไปได้ว่าตัวก่อการการจารกรรมไซเบอร์บางตัวนั้นได้เปลี่ยนวิธีการเป้าหมายจากการพัฒนาทูลที่ตรวจจับยาก (ว่าเป็นมัลแวร์) มาสู่วิธีการวางแผนและดำเนินปฏิบัติการที่มีความซับซ้อน ซึ่งอาจจะไม่จำเป็นต้องเกี่ยวข้องกับมัลแวร์ประเภทที่มีความซับซ้อน แต่ก็ยังคงเป็นมัลแวร์ที่เป็นอันตรายอยู่นั่นเอง” อเล็กซี่ ชูลมิน นักวิเคราะห์มัลแวร์ระดับสูง แคสเปอร์สกี้ แลป กล่าว

และเพื่อเป็นการป้องกันโครงสร้างพื้นฐานไอทีขององค์กรให้พ้นจากการเป็นเป้าหมายการโจมตีของ Microcin ผู้เชี่ยวชาญจากแคสเปอร์สกี้ แลปแนะนำว่าควรติดตั้งซีเคียวริตี้ทูลเพื่อตรวจจับปฏิบัติการไม่พึงประสงค์ แทนที่จะมุ่งตรวจจับแต่เพียงซอฟท์แวร์ไม่พึงประสงค์แต่เพียงเท่านั้น

โซลูชั่นที่สามารถตรวจจับในขั้นซับซ้อนเช่นนั้นได้ อาทิ Kaspersky Anti-Targeted Attack Platform ประกอบด้วยเทคโนโลยีป้องกันระดับเอนด์พอยนท์ และเทคโนโลยีสนับสนุนการติดตามร่องรอยและหาความเชื่อมโยงกันระหว่างอีเว้นท์ที่ปรากฏอยู่บนระบบเครือข่ายในส่วนต่างๆ ขององค์กร เพื่อระบุหารูปแบบประสงค์ร้ายซึ่งเป็นการคุกคามแบบมีเป้าหมาย ที่มักมีความซับซ้อน ได้อีกทางหนึ่ง

ผลิตภัณฑ์ของแคสเปอร์สกี้ แลปสามารถตรวจจับและบล็อกกั้น Microcin และแคมเปญในลักษณะเดียวกันนี้ได้เป็นผลสำเร็จ

รายละเอียด Microcin campaign รวมทั้งข้อมูลด้านเทคนิคต่างๆ ได้ที่

A simple example of a complex cyberattack