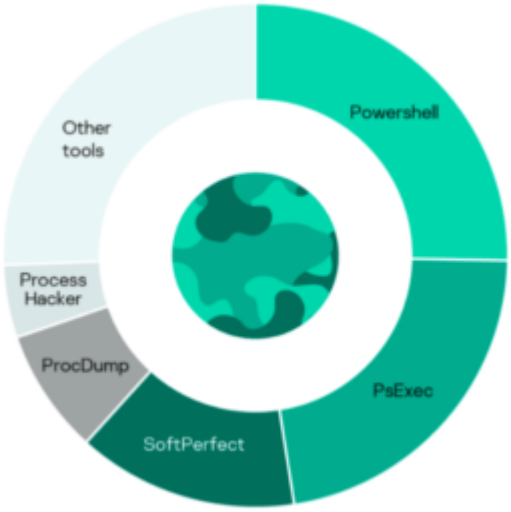
เนียนได้อีก! แคสเปอร์สกี้เผยโจรไซเบอร์แอบใช้ทูลระยะไกลเพื่อโจมตีสำเร็จมากถึง 30%



จากรายงานวิเคราะห์การสนองตอบต่อเหตุการณ์ที่ไม่พึงประสงค์ของแคสเปอร์สกี้ (Incident Response Analytics Report) พบว่า ในปี 2019 บรรดาภัยคุกคามไซเบอร์ที่สืบสวนโดยทีม Kaspersky Global Emergency Response จำนวนเกือบหนึ่งในสาม (30%) เกี่ยวข้องกับทูลการบริหารจัดการระยะไกลที่ถูกกฎหมาย (remote management and administration tools) ทำให้ผู้คุกคามยังคงหลบเลี่ยงการตรวจจับ และลอยนวลอยู่ได้เป็นเวลานานขึ้น อย่างเช่น การก่อจารกรรมไซเบอร์อย่างต่อเนื่องและโจรกรรมข้อมูลลับ มีค่าเฉลี่ยจำนวนวันปฏิบัติการอยู่ที่ประมาณ 122 วัน

ซอฟต์แวร์เฝ้าระวังและบริหารจัดการช่วยให้ผู้ดูแลระบบเครือข่ายและไอทีปฏิบัติงานได้ในแต่ละวัน เช่น แก้ปัญหาและให้การช่วยเหลือพนักงานในองค์กรด้านเทคนิคยามเกิดขัดข้อง อย่างไรก็ตาม อาชญากรไซเบอร์สามารถที่จะหาทางแฝงกายใช้ประโยชน์จากทูลที่ถูกกฎหมายเหล่านี้ได้ ระหว่างที่เกิดเหตุการณ์คุกคามไซเบอร์ขึ้นบนโครงสร้างระบบขององค์กรนั้นๆ ซอฟต์แวร์นี้เปิดช่องให้ผู้ร้ายรันโปรเซสบนเอ็นด์พอยต์ แอคเซส และคอยดึงข้อมูลที่มีความอ่อนไหวออกมาต่างหาก หลบเลี่ยงจุดคุมความปลอดภัยต่างๆ ที่คอยดักจับมัลแวร์

กล่าวโดยรวมแล้ว การวิเคราะห์ข้อมูลส่วนบุคคลในฐานข้อมูลที่ได้รับการปกปิดเพื่อความปลอดภัย (anonymized data) จากการตอบสนองต่อเหตุการณ์ (Incident Response – IR) ต่างๆ พบว่าผู้บุกรุกได้อาศัยประโยชน์จากทูลต่างๆ ที่ถูกต้องเหล่านี้ถึง 18 ทูลด้วยกันในการกระทำการละเมิดระบบ ที่พบใช้กันมากที่สุด ได้แก่ PowerShell (25% ของกรณีที่พบ) เป็นทูลเพื่อการบริหารเครือข่ายที่ถูกใช้เพื่อวัตถุประสงค์ต่างๆ อาทิ รวบรวมข้อมูลเพื่อรันมัลแวร์ และพบ PsExec ถูกใช้อยู่ที่ 22% ของการคุกคาม คอนโซลแอปพลิเคชั่นนี้ถูกใช้เพื่อปล่อยโปรเซสให้ทำงานบนเอ็นด์พอยต์ระยะไกล ตามด้วย SoftPerfect Network Scanner (14%) ซึ่งถูกใช้เพื่อดึงเอาข้อมูลเกี่ยวกับสภาพแวดล้อมของเครือข่าย

เป็นการยากสำหรับซีเคียวริตี้โซลูชั่นในการตรวจจับการเข้าจู่โจมที่ดำเนินการโดยทูลที่ใช้งานอย่างถูกต้อง เพราว่าการกระทำเช่นนี้อาจจะเป็นทั้งส่วนหนึ่งของแผนการของอาชญากรรมไซเบอร์ หรือกิจกรรมงานปกติของผู้ดูแลระบบก็ได้ เช่น ในส่วนของการเข้าโจมตีที่กินเวลาเดือนกว่านั้น เหตุการณ์ไซเบอร์นั้นกินเวลาประมาณ 122 วัน และเนื่องจากไม่ถูกตรวจจับ อาชญากรไซเบอร์จึงได้ทำการเก็บรวบรวมข้อมูลอ่อนไหวสำคัญของเหยื่อไปได้ด้วย

อย่างไรก็ตาม ผู้เชี่ยวชาญของแคสเปอร์สกี้ได้สังเกตว่าบางครั้งแอคชั่นที่ไม่พึงประสงค์บนซอฟต์แวร์ที่ถูกต้องนั้นก็เผยตัวตนออกมาได้รวดเร็ว เช่น ผู้ร้ายมักใช้กับแรนซั่มแวร์ และความเสียหายก็จะชัดเจน ระยะเวลาในการเข้าโจมตีเพียงหนึ่งวัน

“เพื่อเลี่ยงการตรวจจับและหลบแฝงตัวอยู่ในระบบเครือข่ายที่ถูกละเมิดให้นานเท่าที่จะนานได้ ผู้บุกรุกมักจะใช้ซอฟต์แวร์ซึ่งพัฒนาสำหรับยูสเซอร์ใช้งานทั่วไป กิจกรรมงานทั่วไปของผู้ดูแลระบบ และตรวจสอบระบบทั่วๆ ไป ซึ่งทูลเหล่านี้จะช่วยให้ผู้บุกรุกสามารถเก็บรวบรวมข้อมูลเกี่ยวกับระบบเครือข่ายของคอร์ปอเรทได้ จากนั้นดำเนินการแบบคู่ขนาน เปลี่ยนค่าซอฟต์แวร์และฮาร์ดแวร์ หรือแม้แต่ดำเนินการประสงค์ร้ายต่างๆ เช่น แฝงใช้ซอฟต์แวร์ที่ถูกต้องมาทำการเข้ารหัสข้อมูลของของลูกค้า เป็นต้น ทำให้ซอฟต์แวร์ที่เรานำมาใช้งานอย่างถูกต้องนั้นกลายมาเป็นตัวช่วยบังผู้บุกรุกให้หลบเร้นพ้นเรดาร์การตรวจจับของนักวิเคราะห์ความปลอดภัยไปเสียได้ มักจะตรวจจับการคุกคามได้หลังจากเกิดความเสียหายไปแล้วเท่านั้น เป็นไปไม่ได้ที่จะตัดทูลเหล่านี้ออกไป ด้วยเหตุผลหลายประการ อย่างไรก็ตาม ระบบการล็อกกิ้งและสอดส่องที่ใช้งานอยู่นั้นจะเป็นส่วนที่ช่วยให้ตรวจจับความเคลื่อนไหวที่ต้องสงสัยบนระบบเครือข่าย และการเข้าโจมตีที่มีความซับซ้อนได้ตั้งแต่ยังอยู่ระยะแรกๆ” คอนสแตนติน ซาโปรนอฟ หัวหน้าฝ่าย Global Emergency Response Team แคสเปอร์สกี้

เพื่อตรวจจับและจัดการกับการโจมตีให้ได้ทันการณ์นั้น มาตรการหนึ่งที่สำคัญ คือ องค์กรนั้นๆ ควรพิจารณาเรื่องการติดตั้ง โซลูชั่นป้องกันเอ็นด์พอยต์และรับมือกับเหตุการณ์ไม่พึงประสงค์ Endpoint Detection and Response solution ที่มีบริการ MDR service ด้วย บริการประเมินคุณสมบัติของโซลูชั่นต่างๆ ที่เรียกว่า MITRE ATT&CK® Round 2 Evaluation – ที่มีข้อมูลที่เป็นกลางประเมินคุณสมบัติโซลูชั่นต่างๆ รวมทั้งบริการจาก Kaspersky EDR and Kaspersky Managed Protection service ก็รวมอยู่ด้วย เป็นบริการที่จะช่วยลูกค้าเลือกโปรดักส์ EDR ที่เข้า

กับความต้องการใช้งานขององค์กรได้ลงตัว ผลลัพธ์ของการประเมิน ATT&CK Evaluation พิสูจน์แล้วว่าโซลูชั่นที่ครอบคลุมครบถ้วนในทุกจุด ไม่ว่าจะเป็นโปรดักส์ซีเคียวริตี้ที่ป้องกันหลายเลเยอร์โดยอัตโนมัติ และบริการสืบค้นไล่ล่าภัยที่เข้าคุกคามเรานั้น ล้วนมีความสำคัญจำเป็นอย่างยิ่งต่อความปลอดภัยของระบบเครือข่ายขององค์กร

เพื่อลดทอนโอกาสที่ซอฟต์แวร์บริหารระบบจากระยะไกลจะถูกลักลอบใช้เป็นเครื่องมือในการเจาะเข้าโครงสร้างเครือข่ายเสียเอง ทางแคสเปอร์สกี้จึงขอแนะนำมาตรการต่างๆ ด้านความปลอดภัยดังต่อไปนี้

- จำกัดแอคเซสในการใช้ทูลเพื่อการบริหารจากระยะไกลที่มาจาก IP addresses นอกโครงสร้างระบบ จำกัดจำนวนเอ็นด์พอยต์ที่สามารถแอคเซสใช้อินเทอร์เฟซของรีโมทคอนโทรล
- ส่งเสริมนโยบายการตั้งรหัสผ่านที่แข็งแกร่ง ของระบบไอทีทุกระบบในองค์กร และการตรวจทานความถูกต้องของรหัสแบบหลายแฟคเตอร์
- ใช้หลักการในการจำกัดสิทธิ์พิเศษให้แก่พนักงานให้น้อยที่สุด และให้สิทธิ์การเข้าถึงข้อมูลสำคัญของบริษัทแก่ผู้ที่จำเป็นต้องใช้ข้อมูลเพื่อการทำงานเท่านั้น

ข้อมูลเพิ่มเติม

- เรียนรู้เพิ่มเติมเกี่ยวกับ Kaspersky EDR
https://www.kaspersky.ru/enterprise-security/endpoint-detection-response-edr
- รายงาน Incident Response Analytics Report
https://securelist.com/incident-response-analyst-report-2019/97974/