แคสเปอร์สกี้ แลป ยกทัพกูรูร่วมเปิดโปงการก่อจารกรรมไซเบอร์ ในงานประชุมไซเบอร์ซีเคียวริตี้ระดับ APAC ครั้งที่ 3

แคสเปอร์สกี้ แลป เผยภัยพิศวงจากการก่อจารกรรมไซเบอร์ที่มีเป้าหมายที่ประเทศต่างๆ โครงสร้างพื้นฐานที่มีความสำคัญอ่อนไหวต่อความเป็นอยู่ และบริษัทธุรกิจในภูมิภาค ในงาน APAC Cyber Security Weekend 2017 ที่ได้จัดขึ้นครั้งนี้เป็นครั้งที่ 3 ที่ภูเก็ต ประเทศไทย

งานประชุมไซเบอร์ซีเคียวริตี้ประจำปีของภูมิภาคนี้ ได้รวมรวมผู้เชี่ยวชาญ กูรูระดับท็อปของแคสเปอร์สกี้ แลป รวมทั้งของวงการมาไว้ที่เดียวกัน เพื่ออัพเดทข้อมูลให้สื่อมวลชนทั่วภูมิภาคจาก 11 ประเทศในงาน APAC Cyber Security Weekend สุดสัปดาห์แห่งความปลอดภัยไซเบอร์ ที่ภูเก็ตนี้ งานประชุมสี่วันไฮไลต์ที่การนำเสนอข้อมูลค้นคว้าวิจัยโดยนักวิจัยด้านความปลอดภัยชั้นนำของบริษัท ที่ต่างมาแชร์ข้อมูล ความจริงที่ค้นพบ และเปิดโปงความเชื่อผิดๆ เกี่ยวกับการก่อจารกรรมไซเบอร์ ภัยที่น่าตระหนกที่ก่อความหวาดกลัวกันทั่วโลก จากนิยายสายลับสู่ความเป็นจริง

“การจารกรรมไซเบอร์เป็นมหันตภัยที่มีมูลค่าความเสียหายสูงมาก มีเป้าหมายที่องค์กรระดับรัฐและองค์กรธุรกิจทั่วโลก แม้แต่กระทั่งประเทศในแถบภูมิภาคเอเชียแปซิฟิก วันนี้แคสเปอร์สกี้ แลป วางเป้าหมายประกาศเรียกร้องให้ผู้คนสนใจตระหนักถึงมหันตภัยนี้กันมากขึ้น เพื่อที่พวกเราจะได้ยกระดับการป้องกันความปลอดภัยให้แก่โครงสร้างไอทีของเราให้แข็งแกร่งยิ่งขึ้น รวมทั้งหันมาป้องกันสาธารณชนกันมากขึ้นด้วย” สเตฟาน นิวไมเออร์ กรรมการผู้จัดการ แคสเปอร์สกี้ แลป เอเชียแปซิฟิก กล่าว

ในงาน APAC Cyber Security Weekend นี้ เราได้จัดผู้เชี่ยวชาญไซเบอร์ซีเคียวริตี้สี่คนจากทีมวิเคราะห์และวิจัยของแคสเปอร์สกี้ แลป หรือ ทีม GReAT (Global Research & Analysis Team) มาแชร์ข้อมูลสุดยอดด้านไซเบอร์ซีเคียวริตี้ของปี และเจาะเน้นสภาพการณ์ การโจมตีแบบระบุเป้าหมาย (targeted attacks) ต่อประเทศในภูมิภาคเอเชียแปซิฟิก ตั้งอดีตถึงปัจจุบัน และวิธีการที่ภาครัฐ ภาคธุรกิจเอกชน รวมทั้งภาคอุตสาหกรรมที่วิตกกังวลในด้านนี้ สามารถที่จะเสริมความแข็งแกร่งให้แก่ระบบป้องกันทางไซเบอร์ของตนได้

วิทาลี คามลุก ผู้อำนวยการทีม GReAT ประจำภูมิภาคเอเชียแปซิฟิก เปิดการประชุมด้วยการยกประเด็นการโจมตีทางไซเบอร์ครั้งใหญ่ๆ ที่เกิดขึ้นทั้งต่อประชาชนทั่วไปและองค์กรเอกชนในช่วงปีที่ผ่านมาในประเทศต่างๆ ทั่วภูมิ

ภาคนี้

“การก่อจารกรรมไซเบอร์ เป็นส่วนย่อยของวิธีการสืบหาข้อมูลความลับในโลกไซเบอร์ จะต้องปฏิบัติการเป็นความลับที่ถูกปกปิดอยู่แล้วโดยธรรมชาติของตัวมันเอง สปายยุคใหม่ไม่ต้องออกแรงเหมือนเจมส์ บอนด์อีกแล้ว สปายยุคนี้ล้วนแล้วแต่เป็นนักพัฒนาซอฟต์แวร์หรือซิสเต็มโอเปอร์เรเตอร์นี่เอง ผลความสำเร็จของพวกเขาอยู่ในความมืดจนกว่าจะถูกค้นพบเปิดโปงโดยนักวิจัย อย่าง ทีมแคสเปอร์สกี้ GReAT ที่สืบค้น แกะรอย และบันทึกหลักฐานข้อมูลเกี่ยวกับพฤติกรรมรูปแบบการปฏิบัติ ผู้ดำเนินปฏิบัติการโจมตีเหยื่อนั้นมิได้เป็นผู้เขียนประวัติศาสตร์เกี่ยวกับอาชญากรรมไซเบอร์ แต่ นักวิจัยต่างหากที่เป็นคนเขียนประวัติศาสตร์ และก็ไม่ได้ได้มาง่ายๆ ด้วยกับการสืบเสาะแกะรอยข้อมูลเพื่อทำประวัติ ลงบันทึก รายละเอียดขั้นตอนโดยละเอียด กว่าจะงานของนักวิจัยแต่ละชิ้นจะสำเร็จออกมาได้ต้องอาศัยความมุ่งมั่นแรงจูงใจและสมาธิจดจ่อสูงมาก และต้องแก้ลอจิกซับซ้อนมากมายหลายขั้นตอนกว่าจะแก้ได้ทีละเปลาะ ซึ่งนี่คือเหตุผลว่าทำไมเรื่องราวการสืบค้นเหล่านี้จึงมีคุณค่าอย่างยิ่ง” วิทาลีอธิบาย รายงานเรื่อง “Measuring the Financial Impact of IT Security on Businesses” ของแคสเปอร์สกี้ แลป ประจำปี 2016 เป็นชิ้นที่มีรายละเอียดการค้นพบการโจมตีแบบมีเป้าหมาย (targeted attacks) รวมไปถึงการจารกรรมไซเบอร์ ที่ถือว่ามีมูลค่าความเสียหายสูงที่สุด การศึกษาวิจัยพบว่าภัยไซเบอร์เหล่านี้สามารถก่อความเสียหายได้ถึง 143,000 เหรียญสหรัฐเมื่อโจมตีธุรกิจขนาดเล็ก และ 1.7 ล้านเหรียญสหรัฐสำหรับองค์กรขนาดใหญ่

แคสเปอร์สกี้ แลป ยังได้ออกรายงาน เรื่อง “Who’s spying on you. No business is safe from cyber-espionage” เกี่ยวกับการจารกรรมไซเบอร์เช่นกัน และต่างก็ย้ำว่าไม่ว่าธุรกิจในภาคส่วนใด ขนาดใดก็ตามต่างมีสิทธิ์ตกเป็นเป้าหมายของการโจมตีแบบมีเป้าหมายนี้ได้กันทั้งนั้น บริษัทที่อยู่ในอันดับ Fortune 500 มีความเสี่ยงเท่าๆ กับที่สตาร์ทอัพมีพนักงานสองคน เพราะต่างก็มีข้อมูลมีค่าทางธุรกิจนั่นเอง

นอกจากความสูญเสียทางการเงินแล้ว ธุรกิจเอกชนและภาครัฐสูญเสียข้อมูลสำคัญ และความเชื่อมั่นของผู้ถือหุ้นและลูกค้าเมื่อตกเป็นเป้าการจารกรรมข้อมูล

ซองซู ปาร์ค นักวิจัยด้านความปลอดภัยอาวุโส ทีม GReAT ประจำเกาหลีใต้ ได้ให้รายละเอียดถึงความสำคัญของบทบาทของโครงสร้างไอทีองค์กรต่อความอ่อนไหวในการถูกจารกรรมไซเบอร์

ปาร์คเป็นนักวิจัยของแคสเปอร์สกี้ แลป ที่เฝ้าติดตามพฤติกรรมความเคลื่อนไหวของกลุ่มจารกรรมไซเบอร์ไฮโปรไฟล์ที่ชื่อ Lazarus เป็นแก๊งค์อาชญากรไซเบอร์ที่เชื่อกันว่าอยู่เบื้อหลังปฏิบัติการธนาคารบังคลาเทศเมื่อปีที่แล้ว เขากล่าวว่า จากการวิเคราะห์พบว่าแก๊งค์นี้อาศัยเซิร์ฟเวอร์หลายตัวตามคอร์ปอเรทใหญ่ๆ เป็นตัวปล่อย (launchers) การโจมตีองค์กรธุรกิจในแบบเดียวกัน

นูชิน ชาบับ นักวิเคราะห์ด้านความปลอดภัยอาวุโส ทีม GReAT จากออสเตรเลีย ได้พูดถึงเบื้องหลัง บุคคล และวิธีการของการก่อจารกรรมไซเบอร์ รวมทั้งเทคนิคการวิเคราะห์หลักฐานที่เหล่านักวิจัยใช้กันอยู่ เพื่อความเข้าใจการ

โจมตี และเปิดโปงผู้ที่อยู่เบื้องหลังได้ชัดเจนขึ้น

“เช่นเดียวกับนักโบราณคดีที่ต้องขุดค้นเก็บรวบรวมหลักฐานชิ้นเล็กชิ้นน้อย ให้ได้ภาพรวมที่ชัดเจน นักวิจัยไซเบอร์ซีเคียวริตี้ต้องตรวจหาร่องรอยที่หลงเหลืออยู่ของเคมเปญ แกะรอยไปจนกว่าจะรวบรวมชิ้นส่วนเล็กน้อยต่างๆ ที่จำเป็นในการมาต่อเป็นภาพใหญ่ เปรียบเทียบหลักฐานระหว่างผู้เชี่ยวชาญด้วยกันเพื่อหาสมมุติฐานของผู้บงการการก่อจารกรรม เป้าหมายที่แท้จริง เทคนิคและช่วงระยะเวลาของการโจมตี ประวัติข้อมูลเก่าๆ ที่เก็บได้ระหว่างการสืบสวนในช่วงหลายปีมานี้ ช่วยเราได้มากในการค้นพบความจริงหรือความเชื่อผิดๆ เกี่ยวกับจารกรรมไซเบอร์ในภูมิภาคเอเชียแปซิฟิก” นูชินกล่าว

ยูริ นาเมสนีคอฟ นักวิเคราะห์มัลแวร์อาวุโส ทีม GReAT แคสเปอร์สกี้ แลป ได้อรรถาธิบายทิศทางของกลุ่มจารกรรมไซเบอร์ที่โฟกัสที่สถาบันการเงินในภูมิภาค โดยใช้แรนซั่มแวร์อันโด่งดังในปัจจุบันเป็นตัวทำเงิน และได้เปิดเผยเทคนิคที่กลุ่มเหล่านี้ใช้ในการบดบังแฝงตัว Wiper จอมทำลายล้างตัวจริง ที่ทำหน้าที่บุกโจมตี จึงดูเผินๆ เสมือนเป็นงานของอาชญากรรมไซเบอร์ทั่วๆ ไป

นอกจากผู้เชี่ยวชาญด้านไซเบอร์ซีเคียวริตี้จากแคสเปอร์สกี้ แลป ที่ได้มาให้รายละเอียดต่างๆ แล้ว ยังมีหมี มิโดริ คุมะ ผู้พิทักษ์ดาต้าอันโด่งดังหรือ “Data Guardian” ก็ได้มาร่วมงาน เป็นครั้งแรกของเธอที่ได้ร่วมงานในภูมิภาคนี้ เพื่อมาเตือนใจอินเทอร์เน็ตยูสเซอร์ทั้งหลายให้ป้องกันข้อมูลของตนให้พ้นเงื้อมมือภัยจากไซเบอร์

วิทยากรรับเชิญ คยงจู กวัก นักวิจัยด้านความปลอดภัย จากทีมวิเคราะห์เหตุฉุกเฉิน (Computer Emergency Analysis Team) จากสถาบันความมั่นคงปลอดภัยทางการเงินแห่งเกาหลี ได้มาพูดเรื่องของ Andariel ตัวก่อการที่มีความเชื่อมโยงกับกลุ่ม Lazarus และอ้างความรับผิดชอบต่อการรั่วไหลข้อมูลบัตรรวมทั้งการลอบถอนเงินผ่านเอทีเอ็มที่เกาหลีใต้

ข้อมูลเพิ่มเติม

- รายงานเรื่อง Measuring the Financial Impact of IT Security on Businesses

    Report: Measuring the Financial Impact of IT Security on Businesses

- รายงาน เรื่อง “Who’s spying on you. No business is safe from cyber-espionage” https://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf