

แคสเปอร์สกี แลป ยกทัพกูรูร่วมเปิดโปงการก่อจ กรรมไซเบอร์ ในงานประชุมไซเบอร์ซีเคียวริตี้ระดับ APAC ครั้งที่ 3



แคสเปอร์สกี แลป เผยภัยพิวงจากการก่อจกรรมไซเบอร์ที่มีเป้าหมายที่ประเทศต่างๆ โครงสร้างพื้นฐานที่มี
ความสำคัญอ่อนไหวต่อความเป็นอยู่ และบริษัทธุรกิจในภูมิภาค ในงาน APAC Cyber Security Weekend 2017
ที่ได้จัดขึ้นครั้งนี้เป็นครั้งที่ 3 ที่ภูเก็ต ประเทศไทย

งานประชุมไซเบอร์ซีเคียวริตี้ประจำปีของภูมิภาคนี้ ได้รวบรวมผู้เชี่ยวชาญ กูรูระดับท็อปของแคสเปอร์สกี แลป รวม
ทั้งของวงการมาไว้ที่เดียวกัน เพื่ออัปเดตข้อมูลให้สื่อมวลชนทั่วภูมิภาคจาก 11 ประเทศในงาน APAC Cyber
Security Weekend สุดสัปดาห์แห่งความปลอดภัยไซเบอร์ ที่ภูเก็ตนี้ งานประชุมสี่วันไฮไลต์ที่การนำเสนอข้อมูล
ค้นคว้าวิจัยโดยนักวิจัยด้านความปลอดภัยชั้นนำของบริษัท ที่ต่างมาแชร์ข้อมูล ความจริงที่ค้นพบ และเปิดโปงความ
เชื่อผิดๆ เกี่ยวกับการก่อจกรรมไซเบอร์ ภัยที่น่าตระหนกที่ก่อความหวาดกลัวกันทั่วโลก จากนิยายสยองลับสู่ความ
เป็นจริง

“การจกรรมไซเบอร์เป็นมหันตภัยที่มีมูลค่าความเสียหายสูงมาก มีเป้าหมายที่องค์กรระดับรัฐและองค์กรธุรกิจทั่ว
โลก แม้แต่กระทั่งประเทศในแถบภูมิภาคเอเชียแปซิฟิก วันนี้แคสเปอร์สกี แลป วางเป้าหมายประกาศเรียกร้องให้
ผู้คนสนใจตระหนักถึงมหันตภัยนี้กันมากขึ้น เพื่อที่พวกเราจะได้ยกระดับการป้องกันความปลอดภัยให้แก่โครงสร้าง
ไอทีของเราให้แข็งแกร่งยิ่งขึ้น รวมทั้งหันมาป้องกันสาธารณชนกันมากขึ้นด้วย” สเตฟาน นิวไมเออร์ กรรมการผู้
จัดการ แคสเปอร์สกี แลป เอเชียแปซิฟิก กล่าว

ในงาน APAC Cyber Security Weekend นี้ เราได้จัดผู้เชี่ยวชาญไซเบอร์ซีเคียวริตี้สี่คนจากทีมวิเคราะห์และวิจัย
ของแคสเปอร์สกี แลป หรือ ทีม GReAT (Global Research & Analysis Team) มาแชร์ข้อมูลสุดยอดด้านไซเบอร์
ซีเคียวริตี้ของปี และเจาะเน้นสภาพการณ์ การโจมตีแบบระบุเป้าหมาย (targeted attacks) ต่อประเทศในภูมิภาค
เอเชียแปซิฟิก ตั้งอดีตถึงปัจจุบัน และวิธีการที่ภาครัฐ ภาคธุรกิจเอกชน รวมทั้งภาคอุตสาหกรรมที่วิตกกังวลในด้าน
นี้ สามารถที่จะเสริมความแข็งแกร่งให้แก่ระบบป้องกันทางไซเบอร์ของตนได้

วิทาลี คามลุก ผู้อำนวยการทีม GReAT ประจำภูมิภาคเอเชียแปซิฟิก เปิดการประชุมด้วยการยกประเด็นการโจมตี
ทางไซเบอร์ครั้งใหญ่ๆ ที่เกิดขึ้นทั้งต่อประชาชนทั่วไปและองค์กรเอกชนในช่วงปีที่ผ่านมาในประเทศต่างๆ ทั่วภูมิภาค

ภาคนี้

“การก่อการกรรรมไซเบอร์ เป็นส่วนย่อยของวิธีการสืบหาข้อมูลความลับในโลกไซเบอร์ จะต้องปฏิบัติการเป็นความลับที่ถูกปกปิดอยู่แล้วโดยธรรมชาติของตัวมันเอง สบายยุคใหม่ไม่ต้องออกแรงเหมือนเจมส์ บอนด์อีกแล้ว สบายยุคนี้ล้นแล้วแต่เป็นนักพัฒนาซอฟต์แวร์หรือซิสเต็มโอเพอร์เรเตอร์นี่เอง ผลความสำเร็จของพวกเขาอยู่ในความมืดจนกว่าจะถูกค้นพบเปิดโปงโดยนักวิจัย อย่าง ทีมแคสเปอร์สกี GReAT ที่สืบค้น แคะรอย และบันทึกหลักฐานข้อมูลเกี่ยวกับพฤติกรรมรูปแบบการปฏิบัติ ผู้ดำเนินปฏิบัติการโจมตีเหยื่อนั้นมิได้เป็นผู้เขียนประวัติศาสตร์เกี่ยวกับอาชญากรรมไซเบอร์ แต่ นักวิจัยต่างหากที่เป็นคนเขียนประวัติศาสตร์ และก็ได้ไม่ได้ได้มาง่าย ๆ ด้วยการสืบเสาะแคะรอยข้อมูลเพื่อทำประวัติ ลงบันทึก รายละเอียดขั้นตอนโดยละเอียด กว่าผลงานของนักวิจัยแต่ละชิ้นจะสำเร็จออกมาได้ต้องอาศัยความมุ่งมั่นแรงจูงใจและสมาธิจดจ่อสูงมาก และต้องแก้ลจิกซับซ้อนมากมายขั้นตอนกว่าจะแก้ได้ที่ละเปลาะ ซึ่งนี่คือเหตุผลว่าทำไมเรื่องราวการสืบค้นเหล่านี้จึงมีคุณค่าอย่างยิ่ง” วิทาลีอิชบาย

รายงานเรื่อง “Measuring the Financial Impact of IT Security on Businesses” ของแคสเปอร์สกี แลป ประจำปี 2016 เป็นชิ้นที่มีรายละเอียดการค้นพบการโจมตีแบบมีเป้าหมาย (targeted attacks) รวมไปถึงการจากรกรรรมไซเบอร์ ที่ถือว่ามีมูลค่าความเสียหายสูงที่สุด การศึกษาวิจัยพบว่าภัยไซเบอร์เหล่านี้สามารถก่อความเสียหายได้ถึง 143,000 เหรียญสหรัฐเมื่อโจมตีธุรกิจขนาดเล็ก และ 1.7 ล้านเหรียญสหรัฐสำหรับองค์กรขนาดใหญ่

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

นอกจากความสูญเสียทางการเงินแล้ว ธุรกิจเอกชนและภาครัฐสูญเสียข้อมูลสำคัญ และความเชื่อมั่นของผู้ถือหุ้น และลูกค้าเมื่อตกเป็นเป้าการจากรกรรรมข้อมูล

ของซู ปาร์ค นักวิจัยด้านความปลอดภัยอาวุโส ทีม GReAT ประจำเกาหลีใต้ ได้ให้รายละเอียดถึงความสำคัญของบทบาทของโครงสร้างไอทีองค์กรต่อความอ่อนไหวในการถูกจากรกรรรมไซเบอร์

ปาร์คเป็นนักวิจัยของแคสเปอร์สกี แลป ที่เฝ้าติดตามพฤติกรรมความเคลื่อนไหวของกลุ่มจากรกรรรมไซเบอร์ ไฮโปรไฟล์ที่ชื่อ Lazarus เป็นแก๊งค์อาชญากรไซเบอร์ที่เชื่อกันว่าอยู่เบื้องหลังปฏิบัติการธนาคารบังคลาเทศเมื่อปีที่แล้ว เขากล่าวว่า จากการวิเคราะห์พบว่าแก๊งค์นี้อาศัยเซิร์ฟเวอร์หลายตัวตามคอร์ปอเรทใหญ่ๆ เป็นตัวปล่อย (launchers) การโจมตีองค์กรธุรกิจแบบเดียวกัน

นูชิน ซาบับ นักวิเคราะห์ด้านความปลอดภัยอาวุโส ทีม GReAT จากออสเตรเลีย ได้พูดถึงเบื้องหลัง บุคคล และวิธีการของการก่อการกรรรมไซเบอร์ รวมทั้งเทคนิคการวิเคราะห์หลักฐานที่เหล่านักวิจัยใช้กันอยู่ เพื่อความเข้าใจการ

โจมตี และเปิดโปงผู้ที่อยู่เบื้องหลังได้ชัดเจนขึ้น

“เช่นเดียวกับนักโบราณคดีที่ต้องขุดค้นเก็บรวบรวมหลักฐานชิ้นเล็กชิ้นน้อย ให้ได้ภาพรวมที่ชัดเจน นักวิจัยไซเบอร์ซีเคียวริตี้ต้องตรวจหาร่องรอยที่หลงเหลืออยู่ของแคมเปญ และรอยไปจนกว่าจะรวบรวมชิ้นส่วนเล็กน้อยต่างๆ ที่จำเป็นในการมาต่อเป็นภาพใหญ่ เปรียบเทียบหลักฐานระหว่างผู้เชี่ยวชาญด้วยกันเพื่อหาสมมุติฐานของผู้บงการการก่อการกรรม เป้าหมายที่แท้จริง เทคนิคและช่วงระยะเวลาของการโจมตี ประวัติข้อมูลเก่าๆ ที่เก็บได้ระหว่างการสืบสวนในช่วงหลายปีมานี้ ช่วยเราได้มากในการค้นพบความจริงหรือความเชื่อผิดๆ เกี่ยวกับจารกรรมไซเบอร์ในภูมิภาคเอเชียแปซิฟิก” นูชินกล่าว

ยูริ นามสเน็คอฟ นักวิเคราะห์มัลแวร์อาวุโส ทีม GREAT แคลสเปอร์สก็ แลป ได้บรรยายทิศทางของกลุ่มจารกรรมไซเบอร์ที่โฟกัสที่สถาบันการเงินในภูมิภาค โดยใช้แรนซัมแวร์อันโด่งดังในปัจจุบันเป็นตัวทำเงิน และได้เปิดเผยเทคนิคที่กลุ่มเหล่านี้ใช้ในการบดบังแฝงตัว Wiper จอมทำลายล้างตัวจริง ที่ทำหน้าที่บุกโจมตี จึงดูเผินๆ เสมือนเป็นงานของอาชญากรรมไซเบอร์ทั่วไป

นอกจากผู้เชี่ยวชาญด้านไซเบอร์ซีเคียวริตี้จากแคลสเปอร์สก็ แลป ที่ได้มาให้รายละเอียดต่างๆ แล้ว ยังมีหมี มิโคริ คูมะ ผู้พิทักษ์ดาต้าอันโด่งดังหรือ “Data Guardian” ก็ได้มาร่วมงาน เป็นครั้งแรกของเธอที่ได้ร่วมงานในภูมิภาคนี้ เพื่อมาเตือนใจอินเทอร์เน็ตยูสเซอร์ทั้งหลายให้ป้องกันข้อมูลของตนให้พ้นเงื้อมมือภัยจากไซเบอร์

วิทยาการรับเชิญ คยองจูก กวัก นักวิจัยด้านความปลอดภัย จากทีมวิเคราะห์เหตุฉุกเฉิน (Computer Emergency Analysis Team) จากสถาบันความมั่นคงปลอดภัยทางการเงินแห่งเกาหลี ได้มาพูดถึงเรื่องของ Andariel ตัวก่อการที่มีความเชื่อมโยงกับกลุ่ม Lazarus และอ้างความรับผิดชอบต่อการรั่วไหลข้อมูลบัตรเครดิตรวมทั้งการลอบถอนเงินผ่านเอทีเอ็มที่เกาหลีใต้

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>