แคสเปอร์สกี้เผยรายงานวิเคราะห์ APT 3 ปฏิบัติการไซเบอร์ร้ายโจมตีไทย

แคสเปอร์สกี้เปิดโปงปฏิบัติการของกลุ่มอาชญากรไซเบอร์ที่ยังดำเนินการอยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ จากการวิเคราะห์พบว่า ปี 2019 เป็นปีที่กลุ่มผู้ร้ายวุ่นวายอย่างหนักในการเริ่มใช้งานทูลโจมตีใหม่ๆ รวมถึงการสองส่องผ่านโมบายมัลแวร์เพื่อทำจารกรรมล่าข้อมูลจากรัฐบาล หน่วยงานการทหาร และองค์กรต่างๆ ทั่วภูมิภาค

นายวิทาลี คามลัก ผู้อำนวยการทีมวิเคราะห์และวิจัย แคสเปอร์สกี้ ภูมิภาคเอเชียแปซิฟิก กล่าวว่า “ภูมิศาสตร์การเมืองนับเป็นหนึ่งในปัจจัยหลักที่จะกำหนดแนวทางภัยคุกคามในภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยในปีที่แล้ว จากจำนวนเคสที่แคสเปอร์สกี้ตรวจสอบการโจมตีแบบ APT ที่พุ่งเป้าหมายที่ภูมิภาคนี้โดยเฉพาะ แสดงให้เห็นว่า สิ่งที่กระตุ้นให้เกิดการโจมตีหลักๆ แล้วคือการรวบรวมข่าวกรองด้านเศรษฐกิจและภูมิศาสตร์การเมือง”

“ภูมิภาคเอเชียตะวันออกเฉียงใต้ประกอบด้วยประเทศที่มีความหลากหลายทางชาติพันธุ์ วิสัยทัศน์ทางการเมือง และการพัฒนาทางเศรษฐกิจ จึงเป็นปัจจัยกำหนดรูปแบบการโจมตีทางไซเบอร์ที่หลากหลายในภูมิภาคนี้ ผู้เชี่ยวชาญได้เห็นว่าผู้โจมตี APT นั้นปฏิบัติการอย่างไรช่วงหลายปีที่ผ่านมา พัฒนาทูลใหม่อย่างไร มีความระมัดระวังมากขึ้น มีความก้าวหน้าทางเทคนิคและกระตือรือร้นไขว่คว้าเป้าหมายที่สูงขึ้น” นายวิทาลีกล่าวเสริม

กลุ่ม APT ที่โจมตีประเทศไทยในปี 2019 และปฏิบัติการต่อเนื่องในปี 2020 นี้

• ฟันนีดรีม (FunnyDream)
ประเทศเป้าหมายในภูมิภาคนี้: ไทย มาเลเซีย ฟิลิปปินส์ เวียดนาม

ช่วงต้นปี 2020 แคสเปอร์สกี้ออกรายงานการสืบสวนแคมเปญการโจมตีที่ชื่อ “FunnyDream” ผู้ร้ายที่ใช้ภาษาจีนในการสื่อสารนี้ดำเนินการร้ายนานอย่างน้อย 2-3 ปี และฝังมัลแวร์ร้ายที่มีความสามารถหลากหลายไว้ โดยตั้งแต่กลางปี 2018 นักวิจัยของแคสเปอร์สกี้ได้สังเกตุเห็นกิจกรรมที่แอคทีฟอย่างต่อเนื่องจากกลุ่มนี้ มีเป้าหมายส่วนหนึ่งเป็นองค์กรรัฐบาลระดับสูงและพรรคการเมืองในประเทศไทย มาเลเซีย ฟิลิปปินส์ และเวียดนาม

แคสเปอร์สกี้รายงานว่า แคมเปญนี้มีทูลจารกรรมไซเบอร์ที่มีความสามารถหลากหลายจำนวนมาก และยังปฏิบัติการอยู่ ยูสเซอร์สามารถดูข้อมูลอัพเดทได้ที่ Kaspersky Threat Portal

• ไซค์เด็ค (Cycldek)
ประเทศเป้าหมายในภูมิภาคนี้: ไทย ลาว ฟิลิปปินส์ เวียดนาม

กลุ่ม APT อีกกลุ่มที่มีเป้าหมายในภูมิภาคเอเชียตะวันออกเฉียงใต้คือ “Cycldek” ที่ใช้ภาษาจีนในการสื่อสาร แม้ว่าเป้าหมายหลักของกลุ่มนี้คือเครือข่ายรัฐบาลของเวียดนามและลาว แต่ก็พบว่ามีสัดส่วนเป้าหมายในประเทศไทย 3% และพบเหยื่อแคมเปญร้ายหนึ่งรายในฟิลิปปินส์ช่วงปี 2018 – 2019

กลุ่ม Cycldeck นั้นรู้จักกันในอีกชื่อว่า Goblin Panda และมีชื่อเสียงทางร้ายในการจารกรรมข้อมูลหน่วยงานรัฐบาล หน่วยงานการทหาร องค์กรพลังงานโดยใช้ PlugX และมัลแวร์ HttpTunnel

• เซโบรซี (Zebrocy)
ประเทศเป้าหมายในภูมิภาคนี้: ไทย มาเลเซีย

กลุ่ม “Zebrocy” เป็นกลุ่ม APT ที่ใช้ภาษารัสเซียซึ่งใช้ทรัพยากรร่วมกับกลุ่ม Sofacy และยังมีความสนใจและเป้าหมายร่วมกัน กลุ่ม Zebrocy ยังใช้โค้ดมัลแวร์ร่วมกับกลุ่ม BlackEnergy/Sandworm และมีเป้าหมายและใช้โครงสร้างพื้นฐานร่วมกับ BlackEnergy/GreyEnergy อีกด้วย

โปรแกรมแบ็กดอร์ Nimcy ของกลุ่มนี้พัฒนาขึ้นจากภาษาโปรแกรมมิ่ง Nimrod/Nim มีเป้าหมายโจมตีหน่วยงานของประเทศไทยและมาเลเซีย โดย Nimcy เป็นคอลเล็คชั่นภาษาใหม่ของกลุ่ม Zebrocy เพื่อใช้พัฒนาฟังชั่นหลักให้แบ็กดอร์ใหม่ๆ

นายโย เซียง เทียง ผู้จัดการทั่วไป แคสเปอร์สกี้ ภูมิภาคเอเชียตะวันออกเฉียงใต้ กล่าวว่า “การค้นพบของแคสเปอร์สกี้เรื่องการเปลี่ยนแปลงของภัยคุกคามในภูมิภาคนี้ แสดงให้เห็นความจำเป็นในการเร่งพัฒนาศักยภาพการป้องกันทางไซเบอร์ขององค์กรทั้งภาครัฐและเอกชนอย่างมาก กลุ่ม APT เหล่านี้มีวิธีการโจมตีแอบแฝงแทรกซึมเพื่อปฏิบัติการจารกรรมไซเบอร์ในภูมิภาค มาตรการความปลอดภัยจึงจะต้องก้าวล้ำกว่าแค่แอนตี้ไวรัสและไฟร์วอลล์ทั่วไป

โดยแคสเปอร์สกี้เชื่อมั่นในโครงสร้างความปลอดภัยไซเบอร์ที่ก่อร่างสร้างขึ้นจากคลังข้อมูลภัยคุกคามเชิงลึกและทันท่วงที”

“การรวมแมชลีนเลิร์นนิ่งเข้ากับความรู้ของมนุษย์ผ่านนักวิจัยทีม GReAT ของแคสเปอร์สกี้ ทำให้เราสามารถติดตามดูการทำงานของกลุ่ม APT ได้มากกว่า 100 กลุ่มทั่วโลกไม่ว่าจะมีต้นกำเนิดจากที่ใดก็ตาม รายงานทางเทคนิคของแคสเปอร์สกี้ทำให้บริษัทธุรกิจต่างๆ รัฐบาลและองค์กรไม่หวังผลกำไรได้เห็นการเปลี่ยนแปลงและทิศทางของภัยคุกคาม ซึ่งในท้ายที่สุดก็จะเป็นแนวทางปรับปรุงการป้องกันของหน่วยงานนั้นๆ ได้ เรายังแบ่งปันข้อมูลภายในวงการ ยกตัวอย่างเช่นการสานสัมพันธ์กับ INTERPOL เพราะเราเชื่อว่าความร่วมมือกันเป็นหนทางที่ดีที่สุดเพื่อก้าวล้ำนำหน้ากลุ่มจารกรรมไซเบอร์” นายโย เชียง เทียง กล่าวเสริม

นักวิจัยของแคสเปอร์สกี้ขอแนะนะมาตรการเพื่อหลีกเลี่ยงการตกเป็นเหยื่อโจมตีโดยผู้ก่อภัยคุกคาม ดังนี้

- ทีมดูแลความปลอดภัยขององค์กร หรือ SOC (Security Operations Center) จะต้องเข้าถึงฐานข้อมูลภัยคุกคามอัจฉริยะล่าสุด Threat Intelligence เพื่ออัพเดทข้อมูลทูล เทคนิค และกลยุทธ์ใหม่ๆ ที่ผู้ก่อภัยคุกคามและอาชญากรไซเบอร์ใช้งาน
- การตรวจจับระดับเอ็นด์พอยต์ การตรวจสอบ การฟื้นฟูให้ทันท่วงที แนะนำให้ใช้โซลูชั่นสำหรับการตรวจจับและตอบสนองโดยเฉพาะ เช่น Kaspersky Endpoint Detection and Response
- การเพิ่มการป้องกันที่จำเป็นสำหรับเครื่องเอ็นด์พอยต์ แนะนำติดตั้งโซลูชั่นระดับองค์กรที่สามารถตรวจจับภัยคุกคามขั้นสูงในเน็ตเวิร์กได้ตั้งแต่เพิ่มเริ่ม เช่น Kaspersky Anti Targeted Attack Platform