

# ไตรมาส 2 ผู้โจมตีใช้การโจรกรรมและการส่งข้อมูล ปลอม ในตะวันออกกลาง



การโจมตีของภัยคุกคามขั้นสูงในช่วงไตรมาส 2 ปี 2562 นี้ ได้รวมไปถึงจำนวนการโจมตีของกลุ่มตะวันออกกลางและเกาหลีใต้อีกด้วย กิจกรรมการโจมตีหลักนั้นจะเน้นไปที่เป้าหมายการล้วงข้อมูลลับทางการเงิน แต่อย่างน้อยก็มีแคมเปญหนึ่งที่ยังคงมีจุดประสงค์เพื่อขโมยข้อมูลที่บิดเบือน โดยในช่วงเดือนพฤษภาคมที่ผ่านมา นักวิจัย Kaspersky ได้วิเคราะห์การรั่วไหลของสินทรัพย์การโจรกรรมทางออนไลน์ที่เป็นของนิติบุคคลอิหร่าน และสามารถสรุปได้ว่าผู้โจมตีที่อยู่เบื้องหลังคือ Hades เป็นกลุ่มที่เชื่อมโยงกับกับกลุ่ม ExPetr ที่โจมตีเมื่อ Winter Olympic Games ปี 2561 กิจกรรมภัยคุกคามเหล่านี้ที่เกิดขึ้นทั่วโลกได้ถูกรวบรวมไว้ในรายงานสรุปข่าวกรองภัยคุกคามรายไตรมาสล่าสุดของ Kaspersky รายงานสรุปข่าวกรองภัยคุกคามรายไตรมาสนั้นได้รวบรวมจากงานวิจัยของ Kaspersky เอง รวมทั้งจากแหล่งอื่น ๆ ด้วย และเน้นการพัฒนาที่นักวิจัยเชื่อว่าทุกคนควรระวัง

ในช่วงไตรมาส 2 ปีนี้ นักวิจัย Kaspersky

ได้สังเกตและเฝ้าดูกิจกรรมของภัยคุกคามที่น่าสนใจในตะวันออกกลาง  
ที่รวมไปถึงรวมชุดของการสินทรัพย์ที่รั่วไหลออนไลน์ในรูปแบบของรหัส  
โครงสร้างพื้นฐาน กลุ่มและรายละเอียดของเหยื่อที่ชัดเจน  
คาดว่าเป็นกลุ่มโจมตีที่พูดภาษาเปอร์เซีย ที่เรียกว่า OilRig และ  
MuddyWater  
การรั่วไหลครั้งนี้มาจากแหล่งที่แตกต่างกันแต่เริ่มทยอยออกมาในแต่ละ

Tech support burden on younger generation results in relationship rifts  
อย่างเว้นช่วงไม่กี่สัปดาห์

ซึ่งการรั่วไหลครั้งที่สามมีข้อมูลปรากฏว่าเป็นชื่อขององค์กรที่เรียกว่า  
“RANA” เผยแพร่เป็นภาษาเปอร์เซียในเว็บไซต์ชื่อว่า “Hidden  
Reality” นักวิจัย Kaspersky ได้วิเคราะห์ข้อมูลต่าง ๆ

โครงสร้างพื้นฐานและเว็บไซต์เฉพาะที่ใช้

ทำให้พวกเขาสรุปได้ว่าการรั่วไหลนั้นเชื่อมต่อไปถึงกลุ่มผู้โจมตีที่เรียกว่า  
Hades ซึ่งเป็นกลุ่มที่อยู่เบื้องหลังการโจมตีที่เรียกว่า OlympicDestroyer  
ในการแข่งขันกีฬาโอลิมปิกฤดูหนาวปี 2561 และไวรัส ExPetr  
และแคมเปญที่ส่งข้อมูลบิดเบือนอีกหลายตัว เช่น  
อีเมลเกี่ยวกับการเลือกตั้งประธานาธิบดี Emmanuel Macron ในปี 2560  
ที่ฝรั่งเศส อีกด้วย

ภัยคุกคามที่โดดเด่นในช่วงไตรมาส 2 ปี 2562 ประกอบด้วย

□ กลุ่มผู้โจมตีชาวรัสเซียยังคงสร้าง ปรับแต่งเครื่องมืออยู่เสมอ  
และเปิดตัวการโจมตีใหม่ ๆ เช่น เมื่อเดือนมีนาคม กลุ่ม Zebrocy  
ปรากฏตัวในการโจมตีในปากีสถานและอินเดีย

โจมตีเจ้าหน้าที่ที่เกี่ยวข้องกับนักการทูตและกองทัพ

รวมถึงยังคงเข้าถึงเครือข่ายรัฐบาลเอเชียกลาง (Central Asian  
government) นอกจากนี้การโจมตีของกลุ่ม Turla

ยังคงโจมตีอย่างต่อเนื่องและพัฒนาเครื่องมืออย่างรวดเร็ว

และตัวอย่างที่เห็นชัดก็คือการโจรกรรมโครงสร้างพื้นฐานจากกลุ่ม  
OilRig

□ กิจกรรมการโจมตีของกลุ่มเกาหลียังคงอยู่ในระดับสูง

ในขณะที่เอเชียตะวันออกเฉียงใต้อื่น ๆ จะเจียบลงกว่าไตรมาสแรก

ซึ่งกลุ่มที่ปฏิบัติการโจมตี ได้แก่ กลุ่ม Lazarus

ที่โจมตีบริษัทให้บริการเกมออนไลน์ในเกาหลีใต้

Tech support burden on younger generation results in relationship rifts

และแคมเปญของกลุ่ม BlueNoroff ที่เป็นกลุ่มย่อยของ Lazarus

เป้าหมายในการโจมตีคือธนาคารในบังคลาเทศ

และซอฟต์แวร์สกุลเงินคริปโต

□

นักวิจัยได้สังเกตแคมเปญที่พุ่งเป้าหมายการโจมตีไปที่รัฐบาลในเอเชีย

ศูนย์กลางโดยกลุ่มชาวจีน ที่ใช้ชื่อว่า SixLittleMonkeys

โดยใช้โทรจันเวอร์ชันใหม่ของ Microcin และ RAT ที่ Kaspersky

เรียกว่า HawkEye

“ในช่วงไตรมาส 2 ปีนี้ ได้เห็นภัยคุกคามที่มีความซับซ้อนมากขึ้น

และเกิดสิ่งใหม่ ๆ บ่อยมากขึ้น

เราได้เห็นผู้โจมตีที่โจรกรรมโครงสร้างพื้นฐานโดยกลุ่มขนาดเล็ก

และกลุ่มอื่นอาจจะใช้ประโยชน์จากชุดของการรั่วไหลออนไลน์ที่กระจาย

ข้อมูลที่บิดเบือนและทำลายความน่าเชื่อถือของสินทรัพย์ที่หลุดออกมา

ซึ่งอุตสาหกรรมด้านรักษาความปลอดภัยต้องเผชิญกับภารกิจที่เพิ่มขึ้นอย่าง

อย่างต่อเนื่อง

และหาข้อเท็จจริงของภัยคุกคามจากข้อมูลข่าวกรองที่เชื่อถือได้

แต่ก็เป็นธรรมดาที่ยังมีภัยคุกคามหรือกิจกรรมบางอย่างที่เรามองไม่เห็น

หรือไม่ได้เข้าใจอย่างชัดเจน

ดังนั้นการป้องกันภัยคุกคามทั้งที่รู้จักและไม่รู้จักยังคงสำคัญสำหรับทุกคน

” วิเชนต์ ดิแอช หัวหน้าทีมวิจัยด้านความปลอดภัยระดับโลก Kaspersky

กล่าว

รายงานแนวโน้มภัยคุกคามขั้นสูง สำหรับไตรมาส 2

สรุปผลการวิจัยของรายงานข่าวกรองภัยคุกคามเฉพาะสมาชิกของ

Kaspersky ซึ่งรวมถึงข้อมูล IOC และกฎ YARA

เพื่อช่วยในการตรวจสอบทางนิติเวชและมัลแวร์

สำหรับข้อมูลเพิ่มเติมกรุณาติดต่อ intelreports@kaspersky.com

เพื่อหลีกเลี่ยงการตกเป็นเหยื่อของการโจมตีโดยภัยคุกคามที่รู้จักหรือ

ไม่รู้จักก็ตาม นักวิจัย Kaspersky แนะนำให้ปฏิบัติตามนี้

Tech support burden on younger generation results in relationship rifts

□ ให้ข้อมูลภัยคุกคาม (Threat Intelligence) แก่ทีม SOC

เพื่อรับทราบความเคลื่อนไหวและอัปเดตข้อมูลของภัยคุกคามและเครื่องมือ  
เทคนิค และวิธีการในการโจมตีใหม่ ๆ จากกลุ่มอาชญากรไซเบอร์

- ใช้โซลูชัน สำหรับการป้องกัน การสืบสวน
- การแก้ไขเหตุการณ์อย่างทันที่ การดำเนินการของโซลูชัน EDR
- ระดับปลายทาง เช่น Kaspersky Endpoint Detection and Response
- 
- การใช้การป้องกันระดับปลายทางใช้โซลูชันความปลอดภัยระดับองค์กร
- การที่ตรวจจับภัยคุกคามขั้นสูงในระดับเครือข่าย อย่างเช่น Kaspersky Anti Targeted Attack Platform
- 
- แนะนำการฝึกอบรมให้เห็นถึงความตระหนักถึงความปลอดภัยและสอน
- ทักษะการปฏิบัติ ตัวอย่างเช่น Kaspersky Automated Security Awareness Platform.
- ติดตามรายงานฉบับเต็มของรายงานแนวโน้มภัยคุกคามขั้นสูง
- สำหรับไตรมาส 2 ปี 2562 ได้ที่ Securelist.

เกี่ยวกับ Kaspersky

Kaspersky เป็นบริษัทด้านความปลอดภัยบนอินเทอร์เน็ตระดับโลก  
ที่ก่อตั้งในปี 1997

ด้วยความเชี่ยวชาญด้านความปลอดภัยที่ได้พัฒนามาอย่างต่อเนื่อง  
จนปัจจุบันเปลี่ยนเป็นโซลูชันความปลอดภัยยุคใหม่

ที่ให้บริการในการป้องกันสำหรับธุรกิจ โครงสร้างพื้นฐาน  
รัฐบาลและลูกค้าทั่วโลก การให้บริการของบริษัทประกอบด้วย

การป้องกันปลายทาง