วันที่ 14 ตุลาคม 2568

แฮกเกอร์ที่เชื่อมโยงกับกลุ่ม CL0P เจาะระบบองค์กรหลายสิบแห่ง ผ่านช่องโหว่ในซอฟต์แวร์ของ Oracle

มีรายงานล่าสุดที่น่าตกใจจาก Google Threat Intelligence Group (GTIG) และ Mandiant ซึ่งเผยแพร่เมื่อวันพฤหัสบดีที่ผ่านมาว่า องค์กรหลายสิบแห่ง อาจได้รับผลกระทบจากการโจมตีแบบ Zero-day ที่เกิดจากช่องโหว่ในซอฟต์แวร์ Oracle E-Business Suite (EBS) โดยการโจมตีครั้งนี้เริ่มขึ้นตั้งแต่วันที่ 9 สิงหาคม 2025

จอห์น ฮัลต์ควิสต์ หัวหน้านักวิเคราะห์ของ GTIG ภายใต้ Google Cloud เตือนถึงขอบเขตของภัยคุกคามว่า “เรายังอยู่ระหว่างการประเมินขอบเขตของเหตุการณ์นี้ แต่เชื่อว่ามีองค์กรหลายสิบแห่งได้รับผลกระทบ” พร้อมย้ำถึงความรุนแรงของอาชญากรรมไซเบอร์ยุคใหม่: “ในอดีต แคมเปญเรียกค่าไถ่ข้อมูลของ Cl0p เคยมีเหยื่อมากถึงหลายร้อยราย และน่าเสียดายที่การโจมตีแบบ zero-day ในวงกว้างแบบนี้ กำลังกลายเป็นเรื่องปกติของอาชญากรรมไซเบอร์”

Zero-day และกลไกการโจมตีระยะแรก

การโจมตีครั้งนี้มีลักษณะบางอย่างที่คล้ายกับกลุ่มแรนซัมแวร์ Cl0p (หรือที่รู้จักในชื่อ Graceful Spider) โดยผู้โจมตีได้รวมช่องโหว่หลายรายการเข้าด้วยกันเพื่อใช้ในการเจาะระบบเป้าหมาย โดยเฉพาะอย่างยิ่ง ช่องโหว่แบบ zero-day ที่มีรหัส: CVE-2025-61882 (คะแนนความรุนแรง CVSS: 9.8): ช่องโหว่ขั้นร้ายแรงใน Oracle EBS ซึ่งถูกใช้เพื่อเจาะเข้าสู่เครือข่ายของเป้าหมายและขโมยข้อมูลสำคัญออกไป

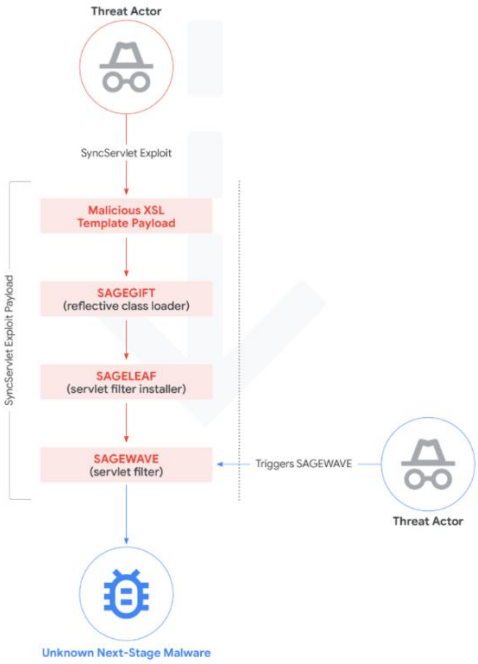
Google พบหลักฐานของกิจกรรมที่น่าสงสัยเพิ่มเติมตั้งแต่วันที่ 10 กรกฎาคม 2025 แล้ว แม้จะยังไม่ทราบว่าการโจมตีในช่วงนั้นสำเร็จมากน้อยเพียงใด แต่ Oracle ได้ออกแพตช์เพื่อแก้ไขปัญหาดังกล่าวแล้ว

เทคนิคขั้นสูง: การรวมช่องโหว่และการฝังมัลแวร์

การโจมตีในครั้งนี้แสดงให้เห็นถึงความทุ่มเททรัพยากรที่สูงมากในการวิจัยและเตรียมการล่วงหน้า โดยมีการใช้ เทคนิคหลายรูปแบบร่วมกัน เพื่อเจาะทะลุระบบป้องกันของ Oracle EBS

เทคนิคการเจาะระบบ (Initial Exploit):

การโจมตีใช้เทคนิคที่ผสมผสานกัน เช่น Server-Side Request Forgery (SSRF), การฉีด CRLF (Carriage-Return Line-Feed), การ ข้ามการตรวจสอบสิทธิ์ (authentication bypass) และการ ฉีดเทมเพลต XSL ซึ่งทั้งหมดนี้มีเป้าหมายเพื่อให้สามารถ รันโค้ดจากระยะไกล (Remote Code Execution) บนเซิร์ฟเวอร์ Oracle EBS และติดตั้ง reverse shell เพื่อควบคุมระบบจากภายนอก



ขั้นตอนการติดตั้งมัลแวร์ (The Payload Drop):

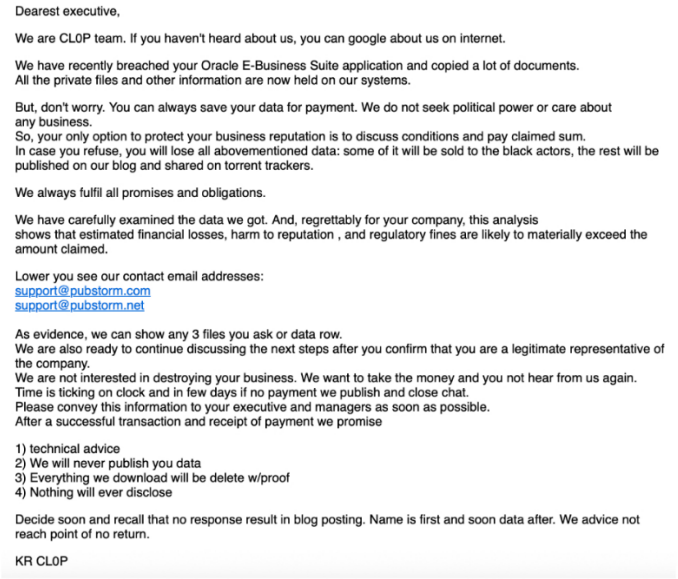
ในช่วงเดือนสิงหาคม 2025 ผู้โจมตีใช้ช่องโหว่ในส่วนประกอบ “/OA_HTML/SyncServlet” เพื่อรันโค้ดจากระยะไกล ผ่านการเรียกใช้ เพย์โหลด XSL โดยฟังก์ชัน Template Preview

ภายในเพย์โหลด XSL นั้นมีเพย์โหลด Java สองชุดที่ซับซ้อน:

- GOLDVEIN.JAVA: เป็นเวอร์ชัน Java ของตัวดาวน์โหลด GOLDVEIN (มัลแวร์ PowerShell ที่ถูกค้นพบครั้งแรกในเดือนธันวาคม 2024 ที่เกี่ยวข้องกับการโจมตีซอฟต์แวร์ของ Cleo) มีหน้าที่รับเพย์โหลดระยะที่สองจากเซิร์ฟเวอร์ควบคุม (C2)

- SAGEGIFT: เป็นโหลดเดอร์ที่เข้ารหัสแบบ Base64 ถูกออกแบบมาสำหรับ Oracle WebLogic โดยเฉพาะ ใช้ในการเปิดตัว SAGELEAF (ตัวติดตั้งในหน่วยความจำ) เพื่อติดตั้ง SAGEWAVE (ฟิลเตอร์ Java Servlet อันตราย ที่ช่วยให้ติดตั้งไฟล์ ZIP เข้ารหัสที่มีมัลแวร์ระยะถัดไปได้ ซึ่งเพย์โหลดหลักนี้มีส่วนคล้ายกับโมดูล “cli” ในแบ็กดอร์ GOLDTOMB ของ FIN11)

นอกจากนี้ ยังพบว่าผู้โจมตีได้รันคำสั่งตรวจสอบระบบ (reconnaissance commands) จากบัญชี “applmgr” ของ Oracle EBS รวมถึงรันคำสั่งจากกระบวนการ bash ที่เปิดจากกระบวนการ Java ที่ทำงานอยู่บน GOLDVEIN.JAVA



Dearest executive,

We are CL0P team. If you haven't heard about us, you can google about us on internet.

We have recently breached your Oracle E-Business Suite application and copied a lot of documents.
All the private files and other information are now held on our systems.

But, don't worry. You can always save your data for payment. We do not seek political power or care about any business.
So, your only option to protect your business reputation is to discuss conditions and pay claimed sum.
In case you refuse, you will lose all abovementioned data: some of it will be sold to the black actors, the rest will be published on our blog and shared on torrent trackers.

We always fulfil all promises and obligations.

We have carefully examined the data we got. And, regrettably for your company, this analysis shows that estimated financial losses, harm to reputation , and regulatory fines are likely to materially exceed the amount claimed.

Lower you see our contact email addresses:
support@pubstorm.com
support@pubstorm.net

As evidence, we can show any 3 files you ask or data row.
We are also ready to continue discussing the next steps after you confirm that you are a legitimate representative of the company.
We are not interested in destroying your business. We want to take the money and you not hear from us again.
Time is ticking on clock and in few days if no payment we publish and close chat.
Please convey this information to your executive and managers as soon as possible.
After a successful transaction and receipt of payment we promise

1) technical advice
2) We will never publish you data
3) Everything we download will be delete w/proof
4) Nothing will ever disclose

Decide soon and recall that no response result in blog posting. Name is first and soon data after. We advice not reach point of no return.

KR CL0P

ความเชื่อมโยงที่น่าสนใจ:

หลักฐานบางส่วนจากเหตุการณ์ในเดือนกรกฎาคม 2025 ที่ได้จากการตอบสนองเหตุการณ์ (incident response) มีความเชื่อมโยงกับโค้ดที่รั่วออกมาในกลุ่ม Telegram ที่ชื่อว่า Scattered LAPSUS$ Hunters เมื่อวันที่ 3 ตุลาคม 2025 อย่างไรก็ตาม Google ระบุว่ายังไม่มีหลักฐานเพียงพอที่จะชี้ว่ากลุ่มนั้นมีส่วนเกี่ยวข้องโดยตรงกับเหตุการณ์นี้

Cl0p/FIN11: กลยุทธ์การเรียกร้องค่าไถ่แบบเงียบและการเปลี่ยนแปลงกลยุทธ์

- รูปแบบการโจมตีล่าสุด: การโจมตีระลอกล่าสุดเริ่มขึ้นอย่างจริงจังเมื่อวันที่ 29 กันยายน 2025 เมื่อผู้โจมตีเริ่มส่งอีเมลจำนวนมากไปยังผู้บริหารของบริษัทต่าง ๆ โดยใช้อีเมลจากบัญชีบุคคลที่สามหลายร้อยบัญชีที่ถูกเจาะมาก่อนแล้ว ซึ่งเชื่อว่าบัญชีเหล่านี้ถูกซื้อมาจากตลาดมืด โดยน่าจะได้มาจากข้อมูลที่ขโมยโดยมัลแวร์ประเภท infostealer
- การเรียกร้องค่าไถ่: ในอีเมลดังกล่าวผู้โจมตีอ้างว่าพวกเขาได้เจาะระบบ Oracle EBS ของเหยื่อและขโมยข้อมูลสำคัญออกไป พร้อมเรียกร้องค่าไถ่เป็นจำนวนเงินที่ไม่ระบุ เพื่อแลกกับการไม่เผยแพร่ข้อมูลที่ขโมยมา แต่จนถึงตอนนี้ยังไม่มีรายชื่อเหยื่อรายใดถูกเผยแพร่ ซึ่งเป็นพฤติกรรมที่สอดคล้องกับรูปแบบการโจมตีของ Cl0p ก่อนหน้านี้ที่มักจะรอเป็นเวลาหลายสัปดาห์ก่อนนำข้อมูลมาเปิดเผย

รอยเท้าของ FIN11 และการวิเคราะห์ของ Google: Google กล่าวเพิ่มเติมว่ายังไม่ได้ยืนยันว่าเป็นการกระทำของกลุ่มที่ติดตามอยู่ใดโดยเฉพาะ แม้จะพบว่ามีการใช้ชื่อ Cl0p ในการโจมตี แต่มีความเป็นไปได้ว่าผู้โจมตีอาจมีความเชื่อมโยงกับกลุ่มนั้น

- เครื่องมือที่คล้ายคลึงกัน: พบว่าเครื่องมือหลังการเจาะระบบ (post-exploitation tooling) มีความคล้ายกับมัลแวร์ GOLDVEIN และ GOLDTOMB ที่เคยใช้ในแคมเปญของ FIN11 มาก่อน
- บัญชีอีเมล: หนึ่งในบัญชีที่ถูกใช้ส่งอีเมลเรียกค่าไถ่ในครั้งนี้เคยถูกใช้โดยกลุ่ม FIN11 ด้วยเช่นกัน

GTIG ระบุว่า “รูปแบบของการโจมตีโดยใช้ช่องโหว่ zero-day ในแอปพลิเคชันที่องค์กรนิยมใช้ และตามมาด้วยการเรียกค่าไถ่ในวงกว้างหลังจากนั้นไม่กี่สัปดาห์ เป็นลักษณะเฉพาะของการโจมตีที่เคยเชื่อมโยงกับกลุ่ม FIN11 ซึ่งเป็นกลยุทธ์ที่ให้ผลลัพธ์สูงและอาจถูกนำไปใช้โดยกลุ่มอื่นได้เช่นกัน”

“การมุ่งเป้าไปยังแอปพลิเคชันหรืออุปกรณ์ที่เปิดให้เข้าถึงจากภายนอก ซึ่งเก็บข้อมูลสำคัญไว้ภายในช่วยให้ผู้โจมตี ‘ขโมยข้อมูล’ ได้มีประสิทธิภาพมากขึ้น เพราะไม่จำเป็นต้องเสียเวลาและทรัพยากรในการเคลื่อนย้ายภายในเครือข่ายขององค์กร ซึ่งเป็นการลงทุนทรัพยากรที่สูง แสดงให้เห็นถึงความทุ่มเทอย่างมากของผู้โจมตีที่อยู่เบื้องหลังการเจาะระบบนี้”

ข้อมูลอ้างอิง

Oct 10, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/10/cl0p-linked-hackers-breach-dozens-of.html