課前研究 - Tracking ShadowHammer

作者:CK

為了讓大家在聽課前先有個小小的概念，我們準備了一個小小小的課前研究課題～不要怕，這個研究課題只是想讓大家分辨自己對情資威脅中的哪一塊比較有興趣。

中文

問題一、[威脅情資報告判讀]－ Operation ShadowHammer 是誰做的？

請讀一下卡巴斯基的報告來理解 Operation ShadowHammer 。根據該份報告，哪一個 APT 族群是此攻擊背後的執行者？

問題二、[系統鑑識]檢查你是否為受害者

有位研究員架設了網站，供大眾檢查自己是否為受害者。請找出網站並檢查你是否受害。

問題三 、[公開來源情資搜尋]華碩電腦何時註銷電子簽章？

華碩電腦在事件發生數月後終於註銷遭竊的電子簽章，而在簽章被註銷前，有一位善良的研究員開設一個推特帳號來追蹤受竊簽章的狀態。請找出這個推特帳號，並檢查華碩何時註銷該電子簽章。

問題四、[逆向工程]逆向惡意程式並找出中繼站

做威脅情報情報的過程中，逆向惡意程式是最~~痛苦~~快樂的時光。請逆向惡意程式並找出中繼站。你可以嘗試使用 Ghidra ！

參考投影片:

一、使用 Ghidra 來逆向 ShadowHammer
https://drive.google.com/file/d/1-qrnc14bfnAwSPkG4rVNscClx2W6GNHD/view?usp=sharing

二、ShadowHammer 樣本
https://drive.google.com/drive/folders/1Me6wy1xGPM-imm_pStJ4FYVdOsG-n184?usp=sharing

英文

Q1. [Threat Report Reading] - Who is behind the Operation ShadowHammer.

Follow and read the report published by Kaspersky, and understand the Operation ShadowHammer. According to the report, which APT group is behind the attacks?

Q2. Check if you are victims

The researcher has constructed a website to check the victims. Find the website and check whether your are targeted?

Q3. [OSINT] When does the ASUS certificate revoke ?

After many days after the attacks happened, ASUS has finally revoked their certificate. A nice researcher made a twitter account to track the certificate. Please find the twitter account and check when the ASUS certificate revoke?

Q4. [Reversing] Find the C2 via reversing the malware.

Reversing malware is the most ~~painful~~ happy time when doing CTI. Please reverse the malware and find the C2. You can try to use Ghidra!

Reference slides:

1. Use Ghidra to reverse ShadowHammer https://drive.google.com/file/d/1-qrnc14bfnAwSPkG4rVNscClx2W6GNHD/view?usp=sharing
2. ShadowHammer sample https://drive.google.com/drive/folders/1Me6wy1xGPM-imm_pStJ4FYVdOsG-n184?usp=sharing

報名連結：**https://forms.gle/nJv7fpnZEiGDNrsx7**
活動介紹：
https://docs.google.com/document/d/1sNEzfj5fLuZTKRVa7xvNovAqHkXY-O5VUJT8BId0bTc/