Petya 變種

勒索病毒 Petya

- Petya 勒索病毒在去年就已出現過。
- 這次新版Petya病毒是利用與WannaCry相同的SMB弱點做滲透並配合WMIC及psexec等RPC工具，對電腦做攻擊。
- 不同點在於：
  - WannaCry僅加密文件，並未加密系統檔案。
  - Petya卻是加密整顆硬碟，讓使用者無從搶救，且即使有SMB的弱點更新，也有可能被感染。

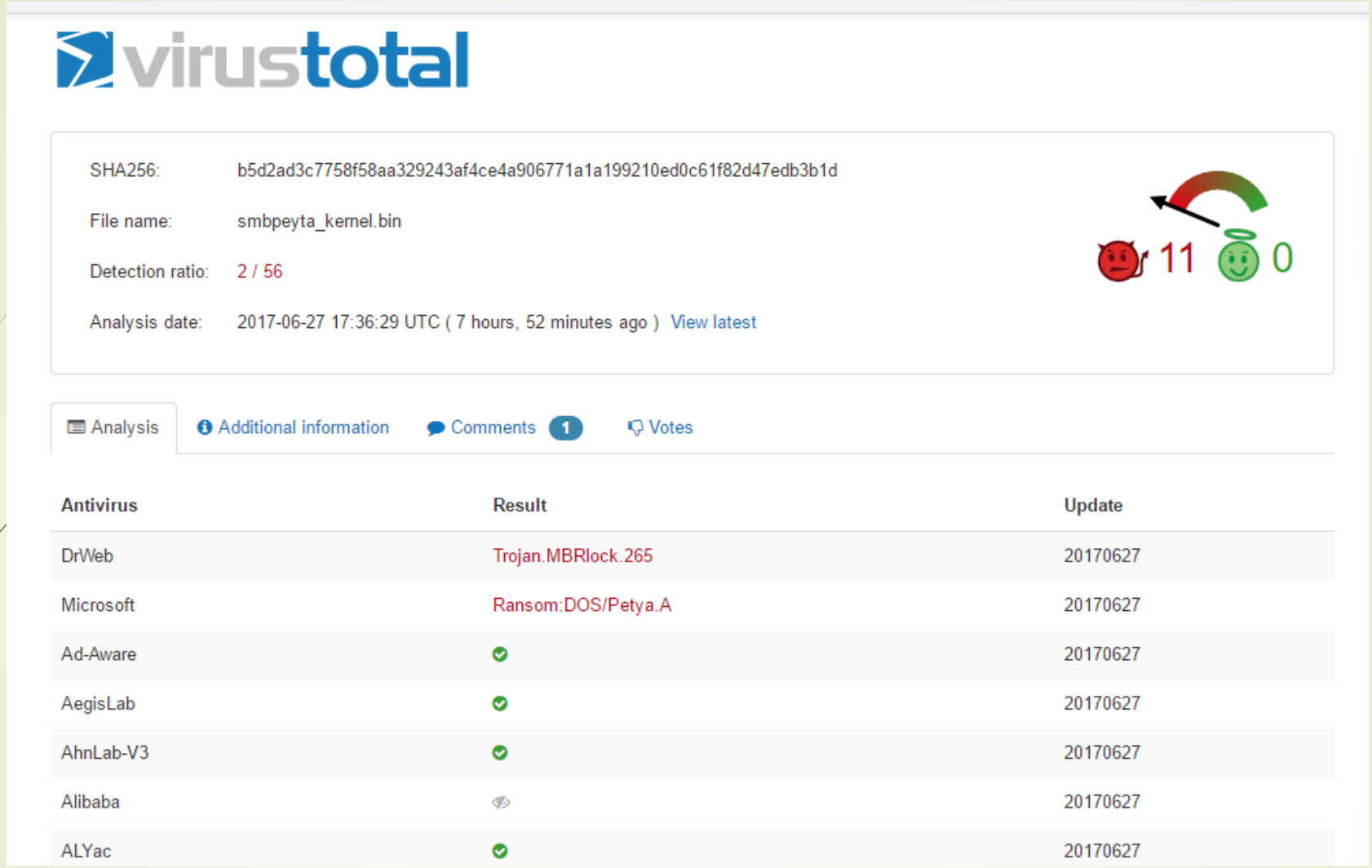
✓ 滲透

- 這次的Petya 勒索病毒是先利用NSA先前外洩的Eternal Blue掃描SMB漏洞，進入受害電腦。

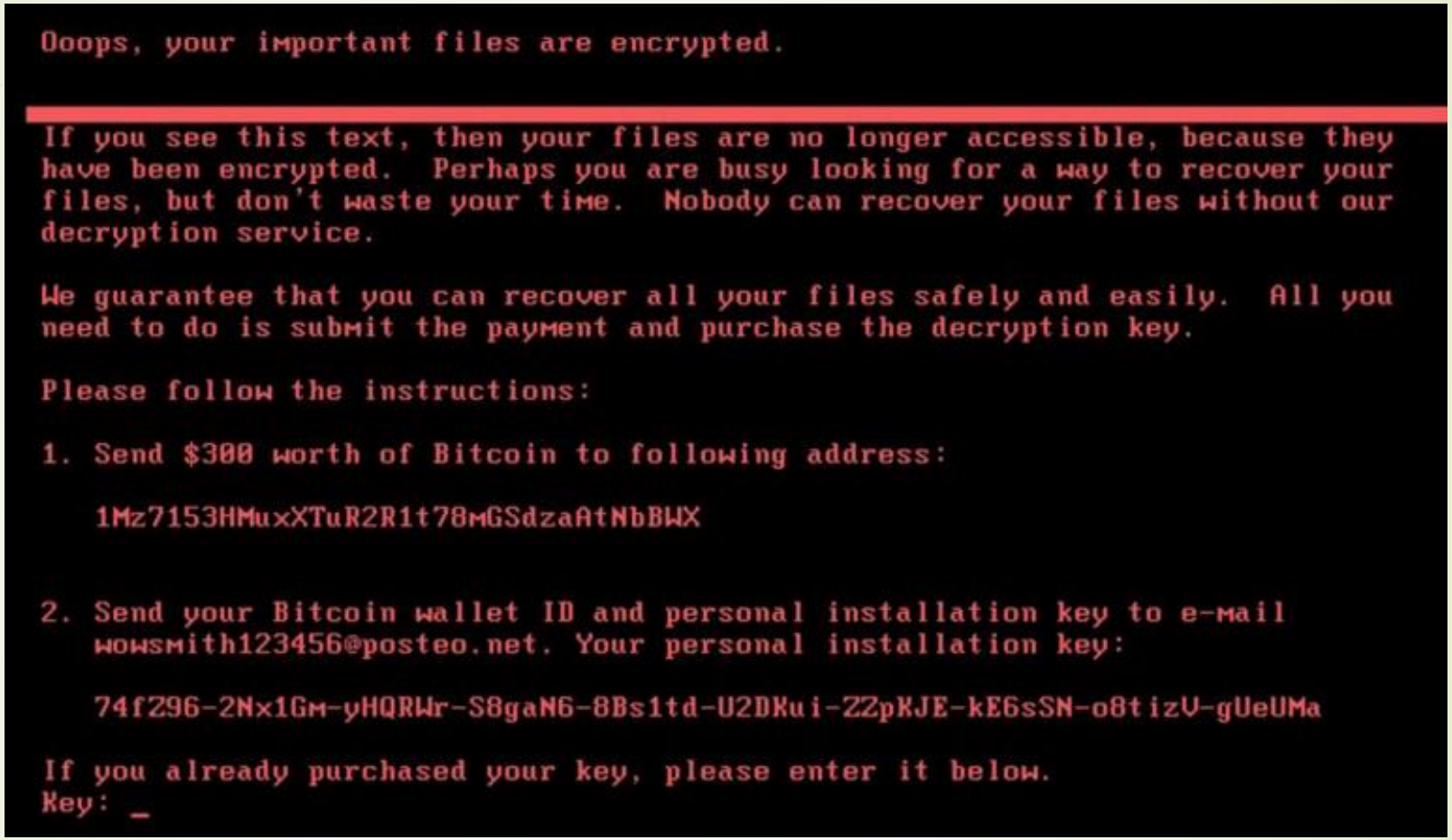
✓ 橫向擴散

- 病毒會先掃描/24的網域IP，將自己複製到有開寫入權限的其他電腦上，並使用PSEXEC在遠端執行。
- 另一種方式是利用WMIC的工具連線至遠端電腦，並竊取帳號資料後，讓病毒能輕易的在其他主機上安裝跟自己一樣的病毒。

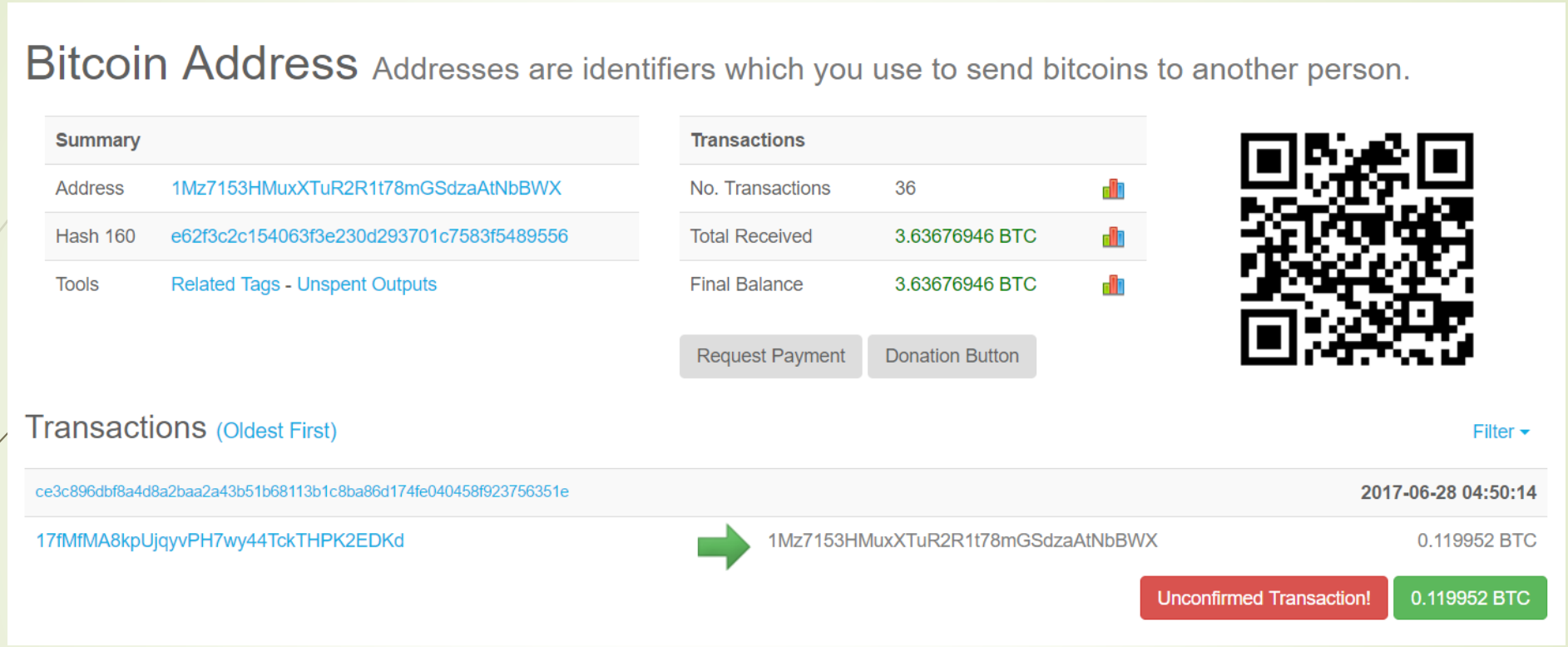
➢ 以上的擴散方法也導致，即便有做WannaCry漏洞更新或是Windows10，只要鄰近的電腦有SMB漏洞，也有被勒索病毒傳染的可能。



有網友將此次的病毒檔，上傳至Virustotal分析，顯示出病毒與先前出現過的Petya病毒有關。



中毒後，所出現的勒索畫面。



在這些Petya勒索軟體中，被發現都指向同一個比特幣位置，截至目前為止(6/28)發現已有36筆交易。

災情：

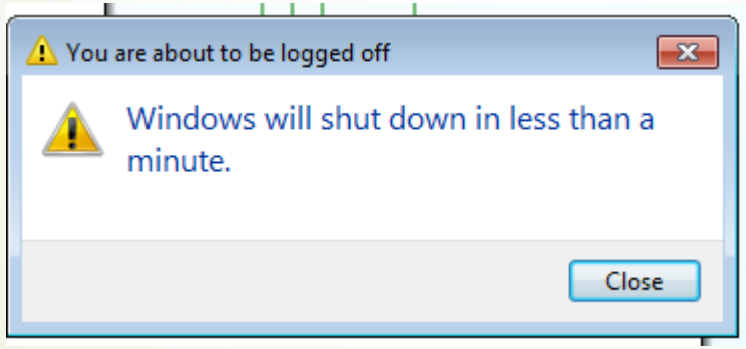
- 俄羅斯、烏克蘭及不少歐洲國家。
- 包含：烏克蘭政府、烏克蘭數間銀行、基輔機場、曾發生過核災的切爾諾貝爾核電廠的輻射監測系統，以及俄羅斯石油 Rosneft 等公家機構及數間企業。
- 德國、法國、挪威、荷蘭以及美國知名大藥廠 Merck 默克及賓州醫院。

預防：

- 使用較複雜的密碼：因Petya有能竊取密碼的機制。
- 安裝 MBRFilter：防止硬碟被更改MBR進行加密。
- 關閉 WMI 服務：防止被Petya進行遠端安裝，但有可能會使RDP遠端服務失效，需小心使用。

緩解方法

- 因Petya進行硬碟加密時，需要重開機，使用者一旦發現無故重開機時，需即刻斷電關機，將硬碟拔至其他電腦進行清理病毒以及備份。



若無故看到這項告警，請即刻關閉電源。

參考資料

- https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html
- https://twitter.com/hasherezade/status/879777725493506050
- https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/
- http://3c.ltn.com.tw/news/30764
- http://technews.tw/2017/06/28/the-global-extortion-virus-recursion-the-petya-variant-is-better-than-the-wannacry-patch/
- https://unwire.hk/2017/06/28/petya/tech-secure/#!prettyPhoto