



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

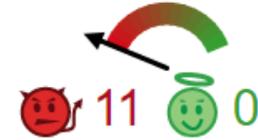
- 病毒會先掃描/24的網域IP，將自己複製到有開寫入權限的其他電腦上，並使用PSEXEC在遠端執行。
- 另一種方式是利用WMIC的工具連線至遠端電腦，並竊取帳號資料後，讓病毒能輕易的在其他主機上安裝跟自己一樣的病毒。
- 以上的擴散方法也導致，即便有做WannaCry漏洞更新或是Windows10，只要鄰近的電腦有SMB漏洞，也有被勒索病毒傳染的可能。

SHA256: b5d2ad3c7758f58aa329243af4ce4a906771a1a199210ed0c61f82d47edb3b1d

File name: smbpeyta\_kernel.bin

Detection ratio: 2 / 56

Analysis date: 2017-06-27 17:36:29 UTC ( 7 hours, 52 minutes ago ) [View latest](#)



Analysis

Additional information

Comments 1

Votes

Antivirus	Result	Update
DrWeb	Trojan.MBRlock.265	20170627
Microsoft	Ransom:DOS/Petya.A	20170627
Ad-Aware	✓	20170627
AegisLab	✓	20170627
AhnLab-V3	✓	20170627
Alibaba	👁	20170627
ALYac	✓	20170627

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。

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:

74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizU-gUeUMa

If you already purchased your key, please enter it below.

Key: \_

中毒後，所出現的勒索畫面。

## Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	<a href="#">1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx</a>
Hash 160	<a href="#">e62f3c2c154063f3e230d293701c7583f5489556</a>
Tools	<a href="#">Related Tags - Unspent Outputs</a>

Transactions		
No. Transactions	36	
Total Received	3.63676946 BTC	
Final Balance	3.63676946 BTC	

[Request Payment](#) [Donation Button](#)



### Transactions (Oldest First)

[Filter](#) ▾

[ce3c896dbf8a4d8a2baa2a43b51b68113b1c8ba86d174fe040458f923756351e](#)

2017-06-28 04:50:14

[17fMfMA8kpUjqyvPH7wy44TckTHPK2EDKd](#)



[1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx](#)

0.119952 BTC

Unconfirmed Transaction!

0.119952 BTC

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。

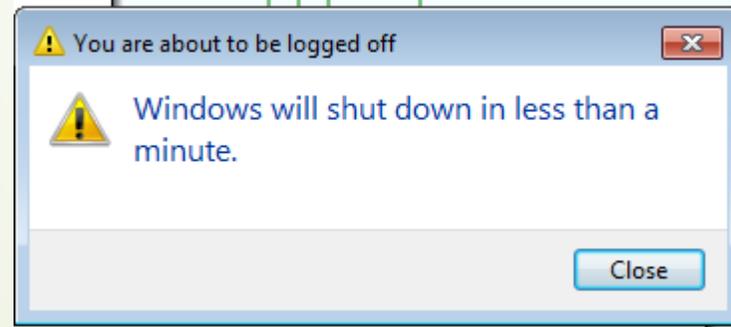


## 預防：

- 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>