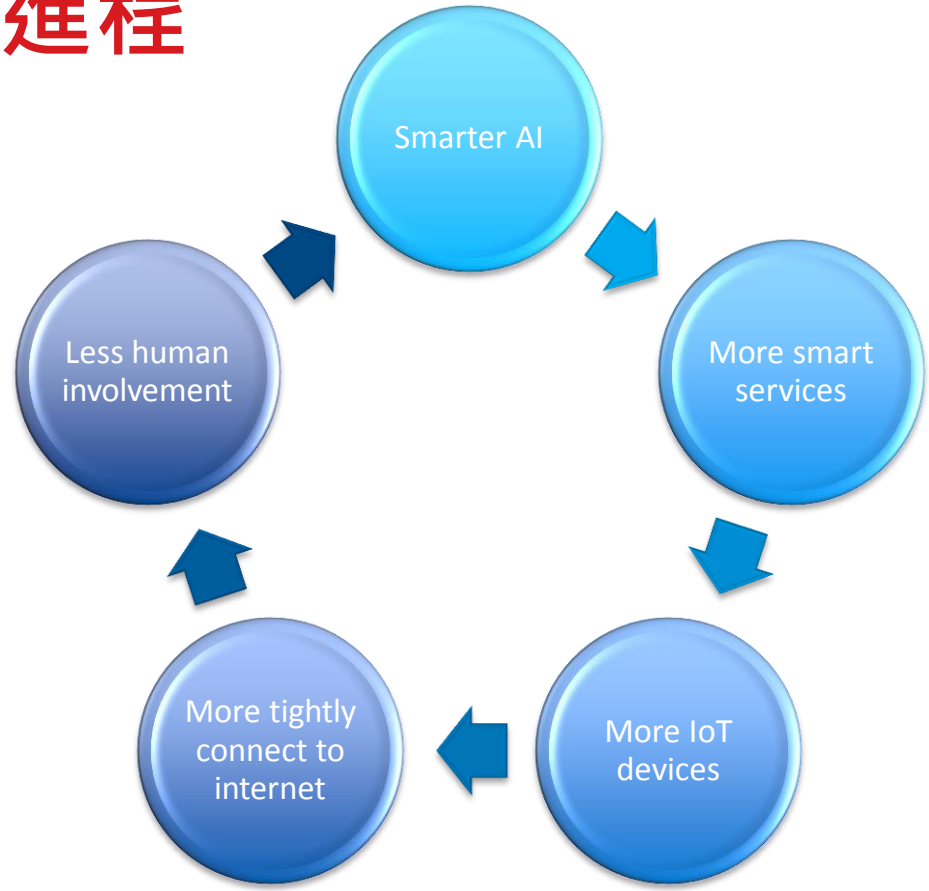
智慧服務的資安挑戰及機會

Bob Hung
Trend Micro TW/HK GM

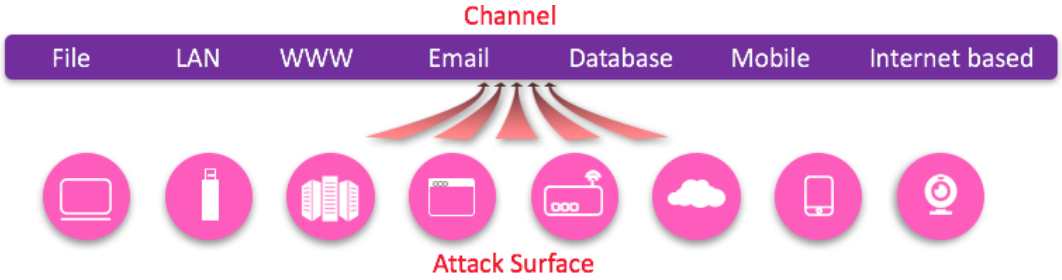
智慧服務的願景

智慧服務進程



駭客眼中的智慧服務

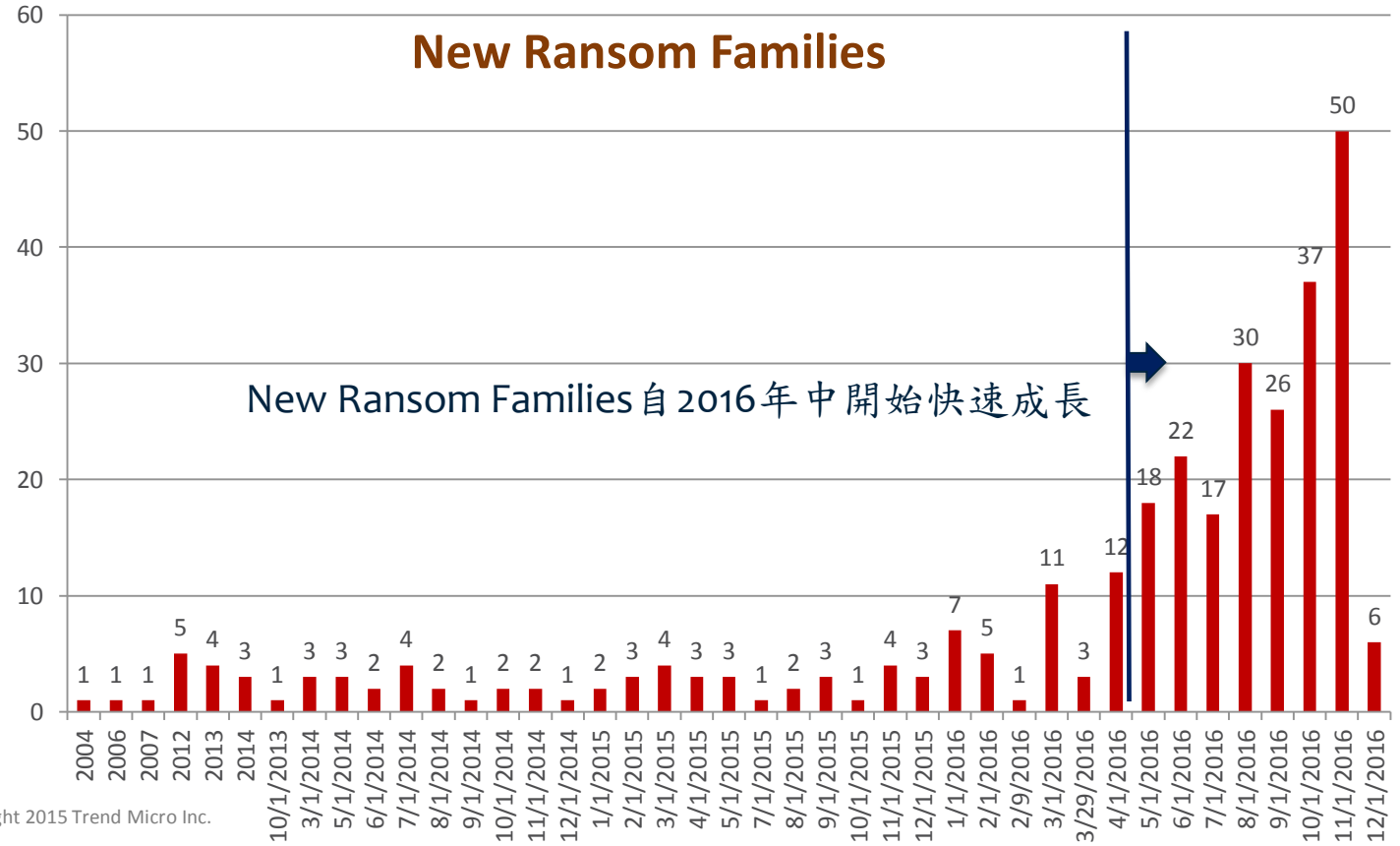
- 更多的攻擊介面
  - IoT 終端、雲端、行動裝置、傳統攻擊介面
- 更易達成的網路勒索
  - 資料損毀（營運中斷）
  - 服務阻絕（營運中斷）
  - 資料污染（營運混亂）
- 更全面的影響
  - 無人化服務
- 更低成本的漏洞開發
  - 駭客的雲端服務



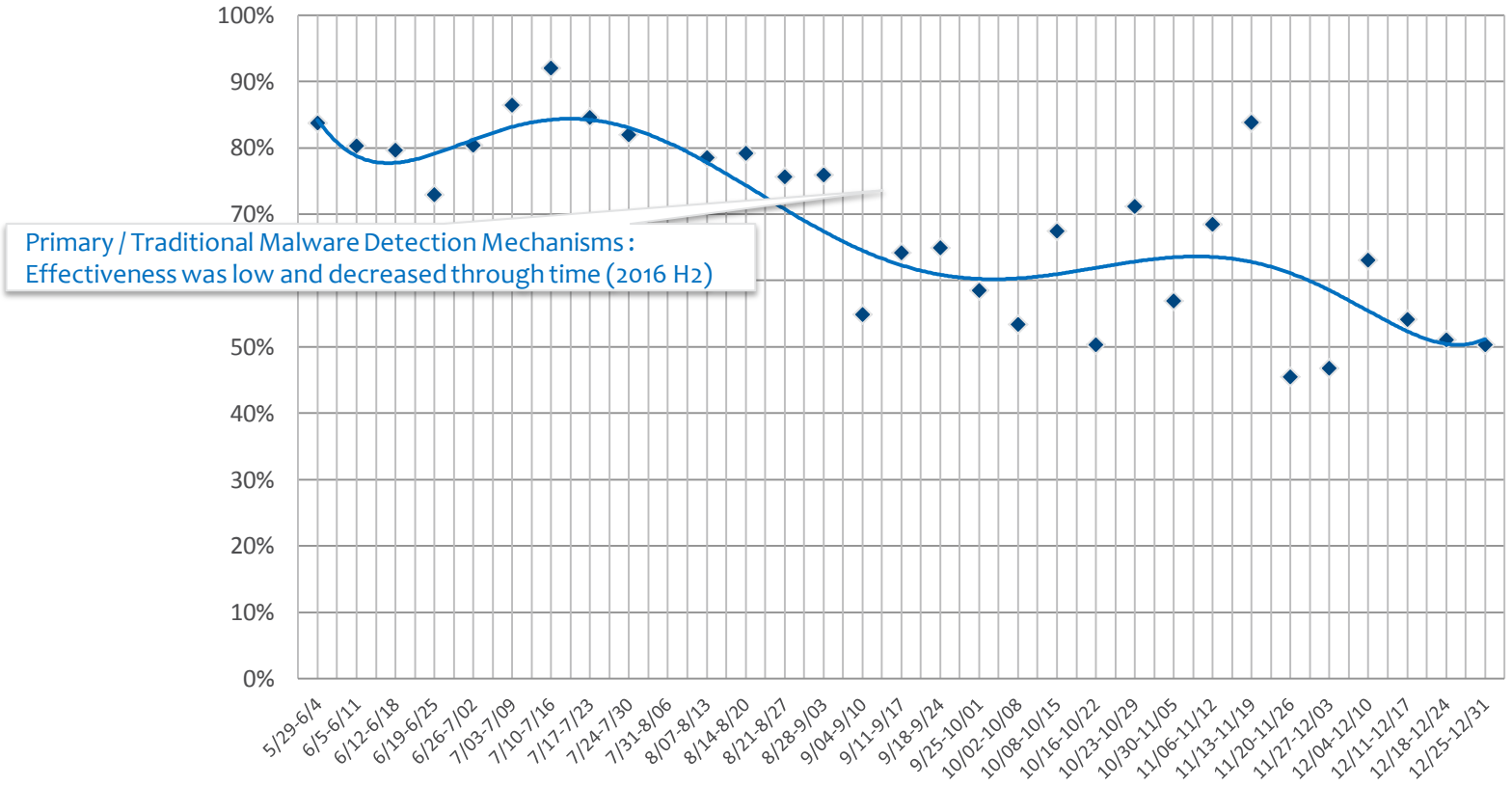
AI 對資安的契機

趨勢科技AI應用案例

資安產業面臨的挑戰（以勒索病毒為例）



傳統偵測技術的侷限



*Source: SPN Feedback (**based on unique sha1**)*

深度學習的應用

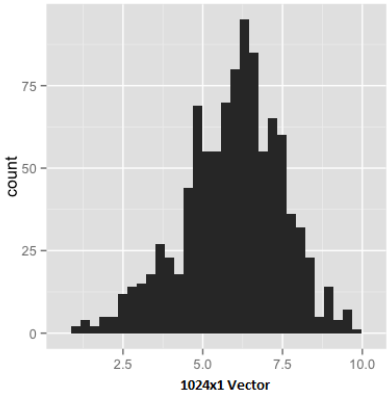
PE File Features – 35 Kinds in Total (1/3)

- Opcode

```
00453820  $  60            PUSHAD
00453821  .  BE 00604400   MOV ESI,35fb2dae.00446000
00453826  .  8DBE 00B0FBFF LEA EDI,DWORD PTR DS:[ESI+FFFB8000]
0045382C  .  57            PUSH EDI
0045382D  .  83CD FF       OR EBP,FFFFFFFF
00453830  .v EB 10         JMP SHORT 35fb2dae.00453842
```

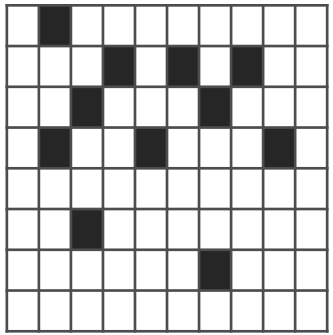
PUSHAD MOV LEA PUSH OR JMP

Unigram



- Import table

FindFirstFile	1
FindNextFile	2
……	……
WriteFileEx	443
Others -> Hash	……

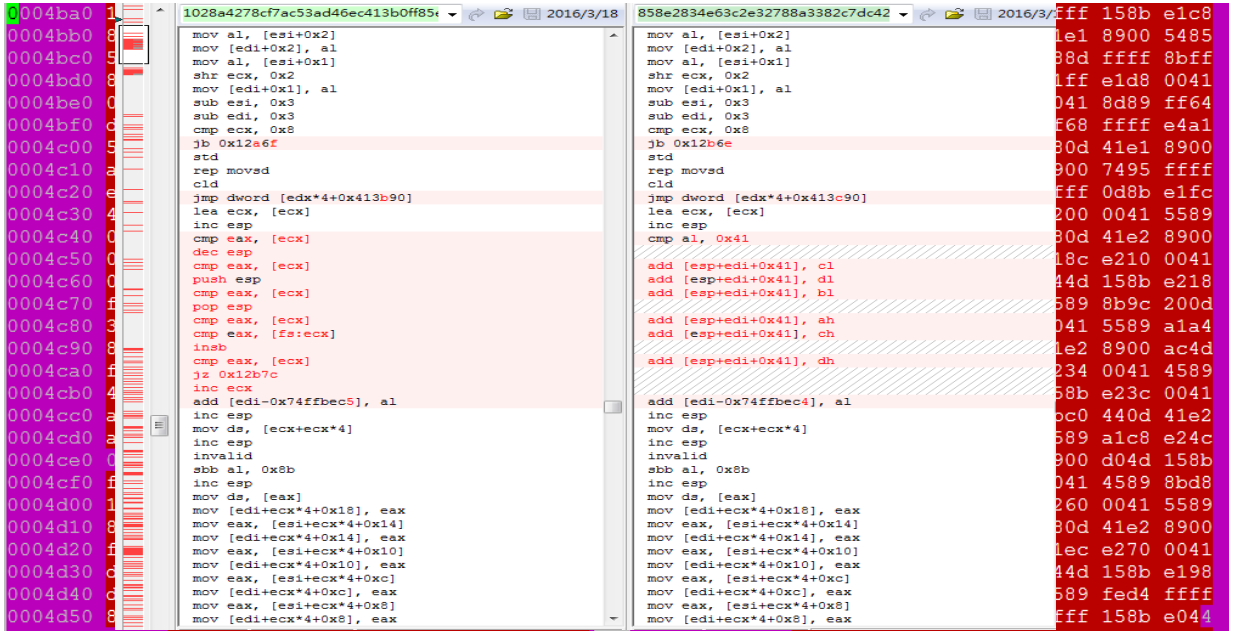


深度學習的應用

PE File Features – 35 Kinds in Total (2/3)

Ransom-Tescrypt
Size: **326144** bytes

Ransom-Tescrypt.H
Size: **196380** bytes

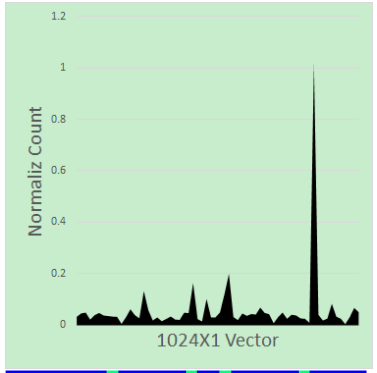
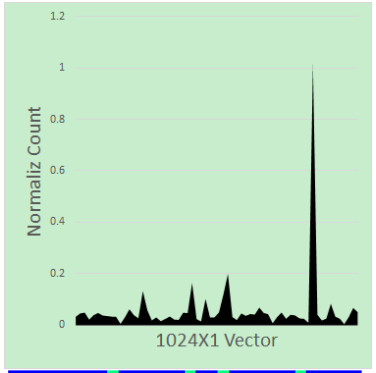
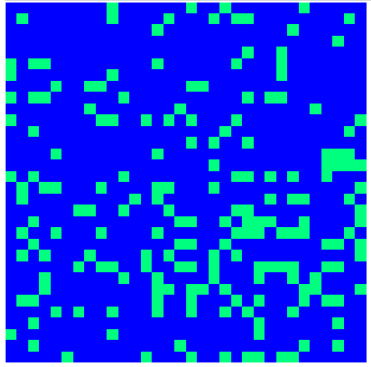
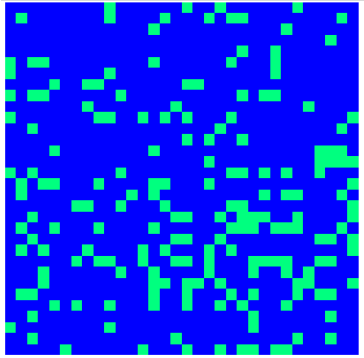


SHA1: 1028a4278cf7ac53ad46ec413b0ff85e45e2c751

SHA1: 858e2834e63c2e32788a3382c7dc427f7aa330c6

深度學習的應用

PE File Features – 35 Kinds in Total (3/3)

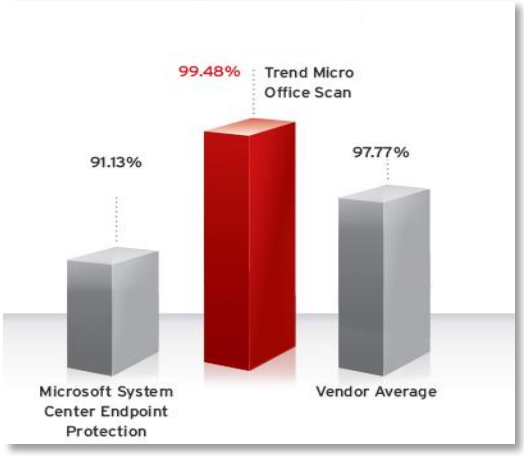
	Ransom-Tescrypt Size: **326144** bytes	**Ransom-Tescrypt.H** Size: **196380** bytes
Opcode		
Import Table		

偵測率的有效提升

Source: Gartner (January 2017)

XGen™

AV-TEST
The Independent IT-Security Institute



TREND MICRO™

Thank you!