

# 智慧服務的資安挑戰及機會

Bob Hung

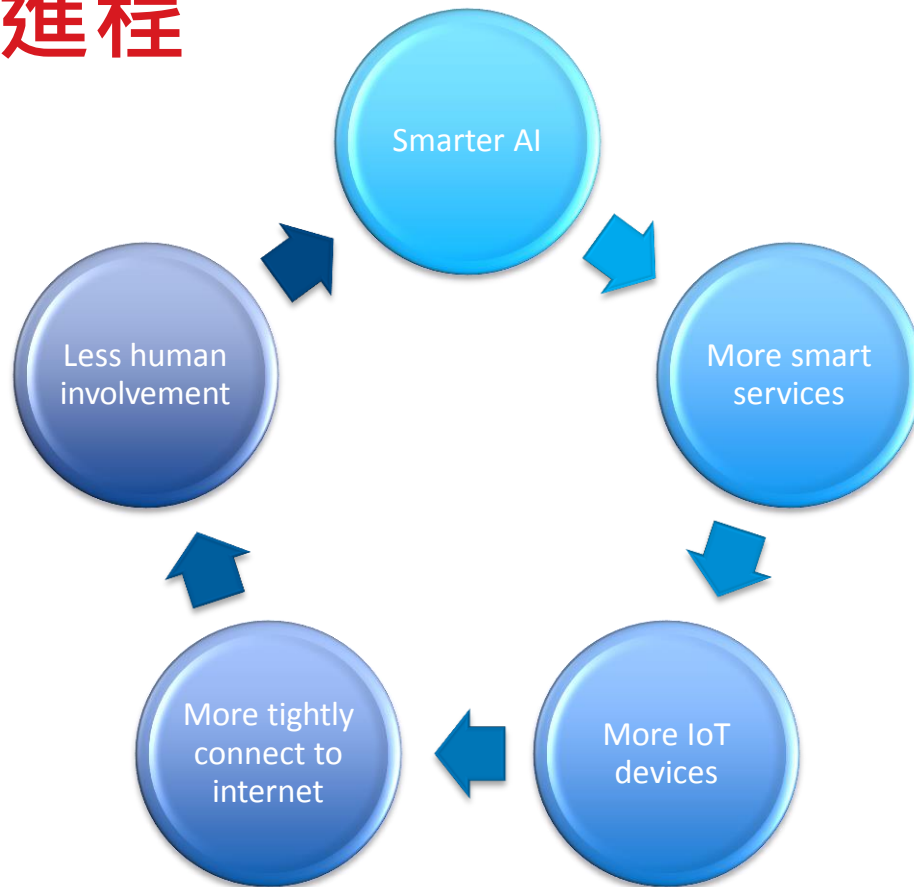
Trend Micro TW/HK GM



# 智慧服務的願景

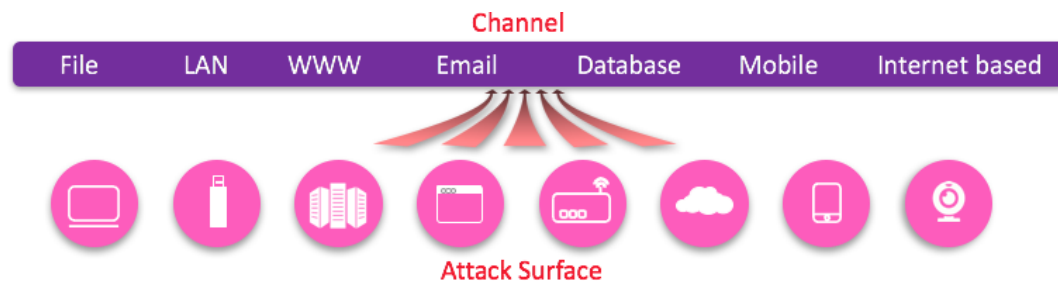


# 智慧服務進程



# 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



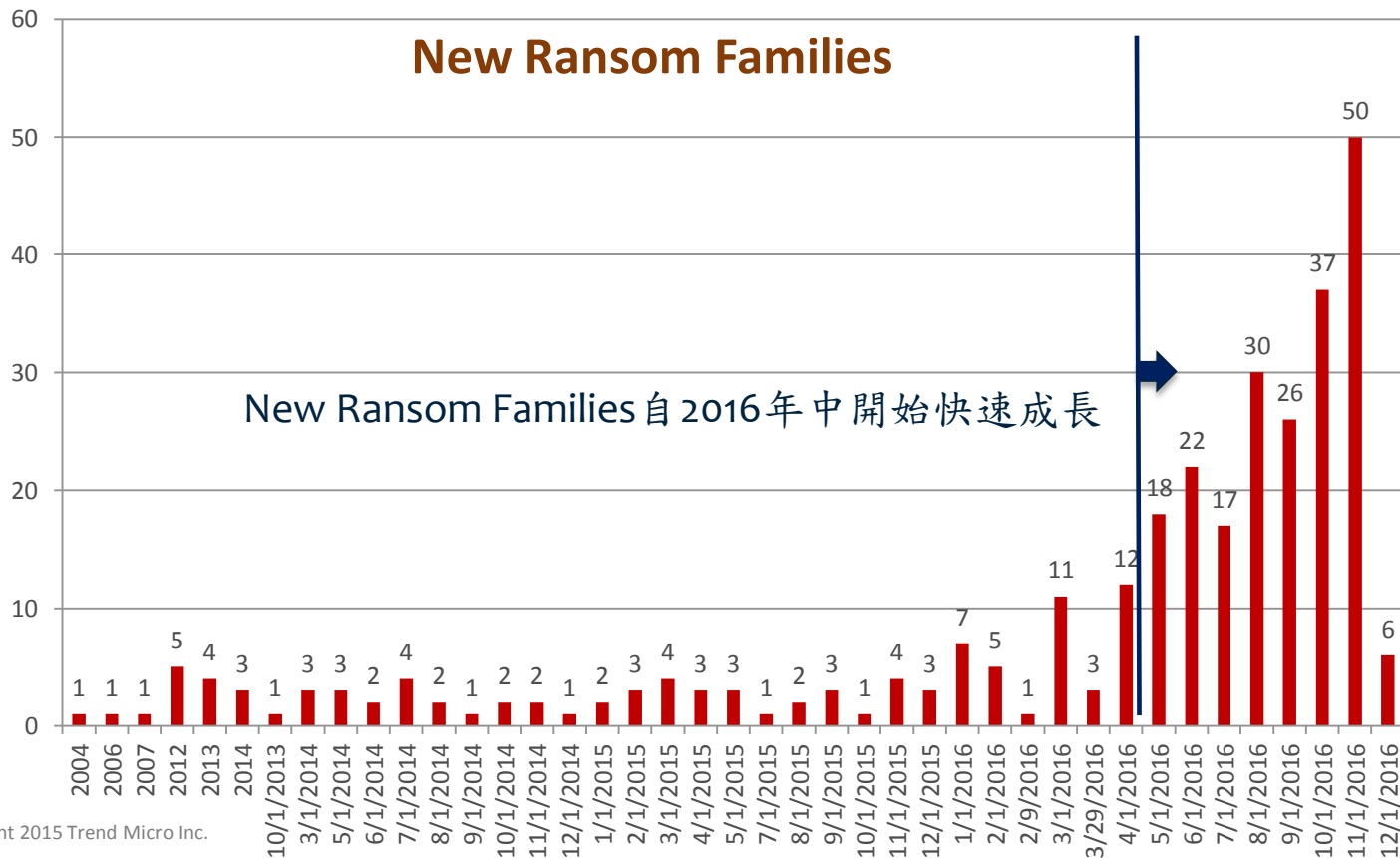
# AI 對資安的契機



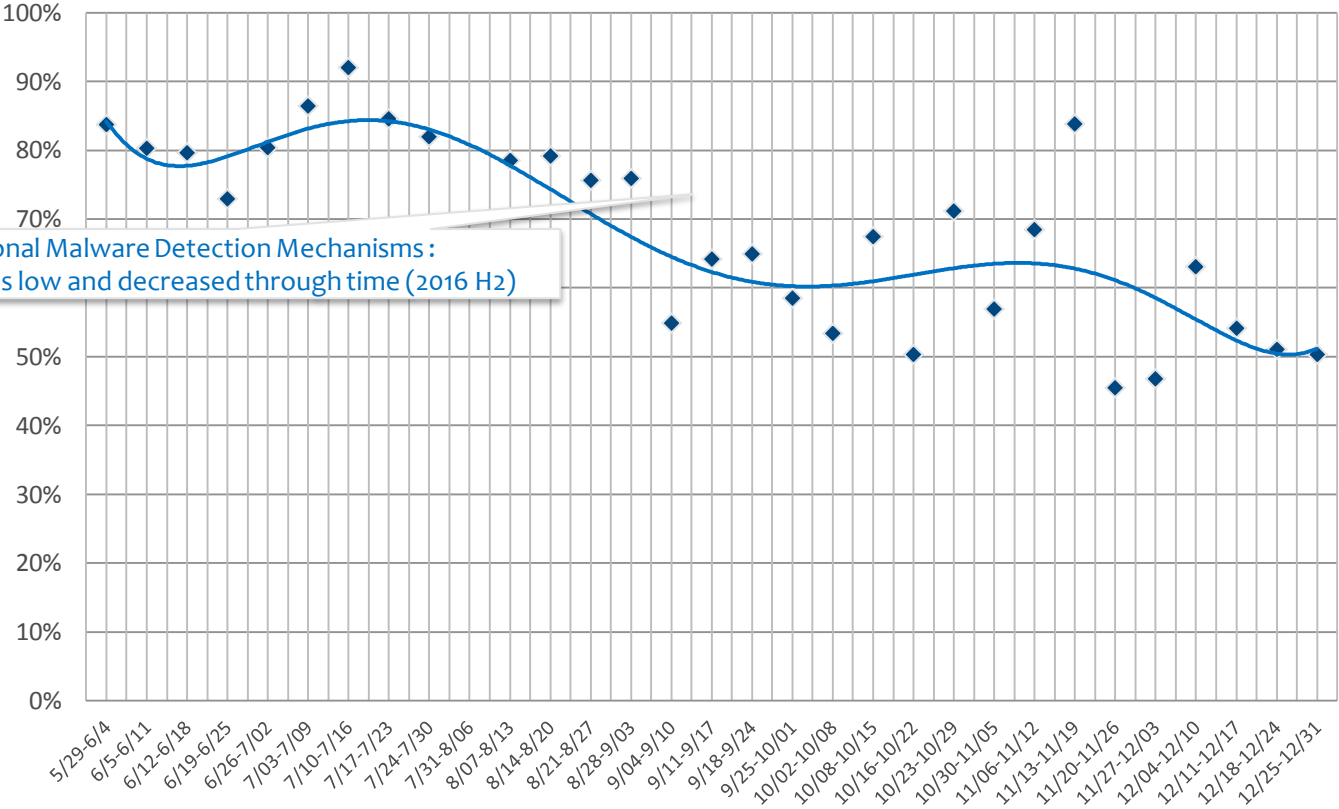
# 趨勢科技AI應用案例

---

# 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



Primary / Traditional Malware Detection Mechanisms: Effectiveness was low and decreased through time (2016 H2)

Source: SPN Feedback (based on unique sha1)



# 深度學習的應用

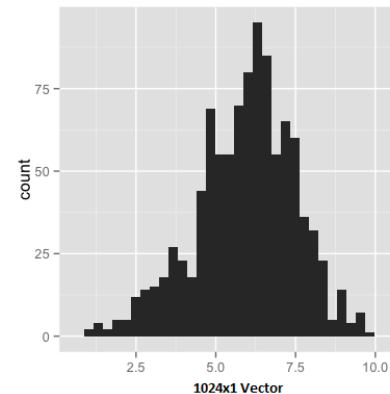
## PE File Features – 35 Kinds in Total (1/3)

- Opcode

```
00453820 $ 60          PUSHAD
00453821 . BE 00604400  MOV ESI,35fb2dae.00446000
00453826 . 8DBE 00B0F8FF LEA EDI,DWORD PTR DS:[ESI+FFF8B000]
0045382C . 57          PUSH EDI
0045382D . 83CD FF     OR EBP,FFFFFFFF
00453830 . EB 10      JMP SHORT 35fb2dae.00453842
```

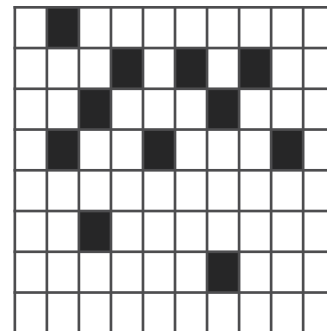
PUSHAD MOV LEA PUSH OR JMP

Unigram



- Import table

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



1024x1 Vector

# 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

```
0004ba0 1 mov al, [esi+0x2]
0004bb0 8 mov [edi+0x2], al
0004bc0 5 mov al, [esi+0x1]
0004bd0 8 shr ecx, 0x2
0004be0 0 mov [edi+0x1], al
0004bf0 c sub esi, 0x3
0004bf0 c sub edi, 0x3
0004bf0 c cmp ecx, 0x8
0004c00 5 jnb 0x12e6f
0004c10 5 std
0004c10 5 rep movsd
0004c20 e cld
0004c30 4 jmp dword [edx*4+0x413b90]
0004c40 4 lea ecx, [ecx]
0004c40 4 inc esp
0004c50 0 cmp eax, [ecx]
0004c60 0 dec esp
0004c70 f push esp
0004c80 3 cmp eax, [ecx]
0004c90 6 insb
0004ca0 4 cmp eax, [ecx]
0004cb0 4 jz 0x12b7c
0004cb0 4 inc ecx
0004cc0 a add [edi-0x74ffbec5], al
0004cd0 a inc esp
0004cd0 a mov ds, [ecx+ecx*4]
0004ce0 a inc esp
0004ce0 a invalid
0004cf0 f sbb al, 0x8b
0004cf0 f inc esp
0004d00 1 mov ds, [eax]
0004d10 1 mov [edi+ecx*4+0x18], eax
0004d20 f mov eax, [esi+ecx*4+0x14]
0004d30 c mov [edi+ecx*4+0x14], eax
0004d40 c mov eax, [esi+ecx*4+0x10]
0004d50 c mov [edi+ecx*4+0x10], eax
0004d50 c mov eax, [esi+ecx*4+0xc]
0004d50 c mov [edi+ecx*4+0xc], eax
0004d50 c mov eax, [esi+ecx*4+0x8]
0004d50 c mov [edi+ecx*4+0x8], eax
```

SHA1: 1028a4278cf7ac53ad46ec413b0ff85e45e2c751

```
858e2834e63c2e32788a3382c7dc42 fff158b e1c8
858e2834e63c2e32788a3382c7dc42 ffe1 8900 5485
858e2834e63c2e32788a3382c7dc42 88d ffff 8bff
858e2834e63c2e32788a3382c7dc42 1ff e1d8 0041
858e2834e63c2e32788a3382c7dc42 041 8d89 ff64
858e2834e63c2e32788a3382c7dc42 f68 ffff e4a1
858e2834e63c2e32788a3382c7dc42 jnb 0x12b6e
858e2834e63c2e32788a3382c7dc42 std
858e2834e63c2e32788a3382c7dc42 rep movsd
858e2834e63c2e32788a3382c7dc42 cld
858e2834e63c2e32788a3382c7dc42 jmp dword [edx*4+0x413c90]
858e2834e63c2e32788a3382c7dc42 lea ecx, [ecx]
858e2834e63c2e32788a3382c7dc42 inc esp
858e2834e63c2e32788a3382c7dc42 cmp al, 0x41
858e2834e63c2e32788a3382c7dc42 add [esp+edi+0x41], cl
858e2834e63c2e32788a3382c7dc42 add [esp+edi+0x41], dl
858e2834e63c2e32788a3382c7dc42 add [esp+edi+0x41], bl
858e2834e63c2e32788a3382c7dc42 add [esp+edi+0x41], ah
858e2834e63c2e32788a3382c7dc42 add [esp+edi+0x41], ch
858e2834e63c2e32788a3382c7dc42 add [esp+edi+0x41], dh
858e2834e63c2e32788a3382c7dc42 add [edi-0x74ffbec4], al
858e2834e63c2e32788a3382c7dc42 inc esp
858e2834e63c2e32788a3382c7dc42 mov ds, [ecx+ecx*4]
858e2834e63c2e32788a3382c7dc42 inc esp
858e2834e63c2e32788a3382c7dc42 invalid
858e2834e63c2e32788a3382c7dc42 sbb al, 0x8b
858e2834e63c2e32788a3382c7dc42 inc esp
858e2834e63c2e32788a3382c7dc42 mov ds, [eax]
858e2834e63c2e32788a3382c7dc42 mov [edi+ecx*4+0x18], eax
858e2834e63c2e32788a3382c7dc42 mov eax, [esi+ecx*4+0x14]
858e2834e63c2e32788a3382c7dc42 mov [edi+ecx*4+0x14], eax
858e2834e63c2e32788a3382c7dc42 mov eax, [esi+ecx*4+0x10]
858e2834e63c2e32788a3382c7dc42 mov [edi+ecx*4+0x10], eax
858e2834e63c2e32788a3382c7dc42 mov eax, [esi+ecx*4+0xc]
858e2834e63c2e32788a3382c7dc42 mov [edi+ecx*4+0xc], eax
858e2834e63c2e32788a3382c7dc42 mov eax, [esi+ecx*4+0x8]
858e2834e63c2e32788a3382c7dc42 mov [edi+ecx*4+0x8], eax
```

SHA1: 858e2834e63c2e32788a3382c7dc427f7aa330c6

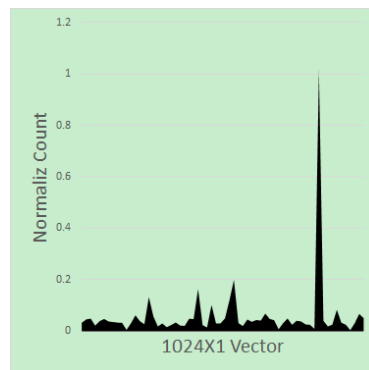
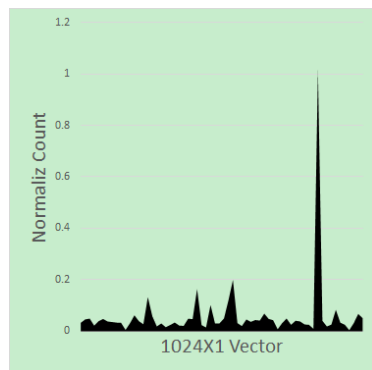
# 深度學習的應用

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

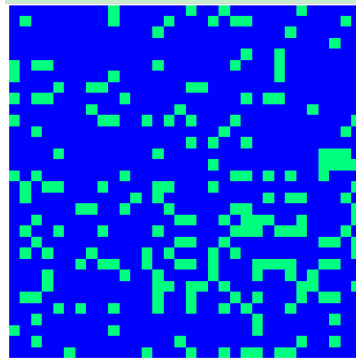
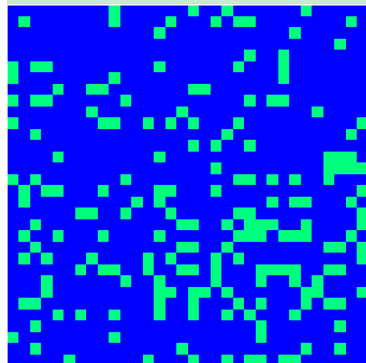
**Ransom-Tescrypt**  
Size: **326144** bytes

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

**Opcode**



**Import  
Table**



# 偵測率的有效提升

2017/26

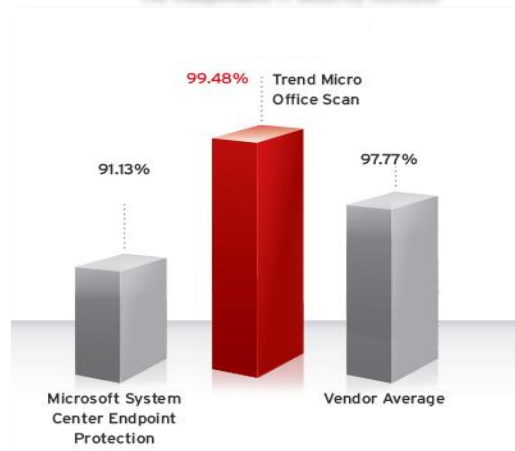
Gartner Reprint



Source: Gartner (January 2017)

# XGen™

**AVTEST**  
The Independent IT-Security Institute



# Thank you!

---