

ArmorX APT 惡意電子郵件防禦

流量清洗·回溯追蹤與連線反制駭客
地表最強·APT 防禦與 BEC 防禦



電子郵件為企業對外開放的主要通訊管道之一，無時無刻不遭受猛烈的 APT 攻擊。這些攻擊會嚴重影響政府、企業與個人的工作環境、財務風險，甚至營運信心。APT 攻擊手段包含 BEC 交易詐騙、加密勒索、操控系統、竊取情資、癱瘓勒索等，APT 攻擊勢力來自各方力量，涵蓋黑道、軍方、國家等，APT 攻擊總額 2017 年起已正式超越全球資安產值，其中 BEC 交易詐騙佔 APT 攻擊總額 50% 以上，受災對象涵蓋政府單位與民間企業，受災者追討無門，在在凸顯自我資安防衛的重要性。

80% 以上 APT 攻擊從電子郵件進入，Mail APT 攻擊防禦成為當前最重要課題。ArmorX 運用最先進 AI 人工智慧與 Cloud 雲端掃描技術，打造地表最強大、最全面 SMTP(s) 四項安全防護：流量清洗、APT 攻擊防禦、BEC 詐騙防禦、(選購) BEC 滲透防禦 (Exchange 安全代理)，能大幅降低攻擊流量與打造最佳安全防線。

流量清洗

APT 集團日益獲利增長與資源擴張，「密碼會被猜中」成為基本假設，「流量清洗」為必要手段。假設駭客成功連線 100 萬次會猜中，阻斷連線 90% 會讓駭客基於成效不彰而轉戰。本系統提供 ArmorX 雲端聯防機制，輔以主動偵測與學習攻擊與滲透來源，制敵防護於封包接收前，大幅降低攻擊與垃圾郵件量。

BEC 詐騙防禦

常見 APT 釣魚信件（假冒知名單位）與 BEC 詐騙信件（假冒廠商）不包含惡意程式，而是用「騙」的。本系統運用假冒、匿名、濫發、非法解析等，強化變臉詐騙防禦，包含假冒自己、外部、知名業者、電信服務業者等，同時降低電子郵件系統遭受中間人收信滲透的風險。

APT 攻擊防禦

本系統運用 AI 人工智慧技術，強化惡意程式行為解析，包含反偵測行為、CVE 弱點漏洞偵測、加密演算行為（勒索病毒）、嵌入漏洞檢查套件、隱藏包裝、文字命令程式等，可執行加密附件本封與他封密碼檢測，(選購) 硬體式動態沙箱鑑識，可強化置換網址連線檢測與排程網址安全檢測。

(選購) 獨家 Exchange 安全代理

BEC 交易詐騙分為兩個階段，滲透階段與詐騙階段，滲透階段主要目的就是取得電子郵件系統內的使用者信件。本系統可作為 Https 與 Exchange 安全代理，支援 ROH、OWA、ActiveSync 等協定，執行流量清洗防止駭客猜密碼與弱掃，以及帳號/群組國別存取控管。

全球獨家專利技術

SMTP 即時回溯追蹤

SMTP 攻擊連線反制

SMTP 通訊行為解析

MUA+MTA 路由

MTA 防偽來源路由

FQDN[IP]/來源國別

雙認證白名單

MTA+Email 或 Domain

3000 萬+

APT 駭客 IP 與短期網域

4000 萬+

已知惡意程式特徵碼



國際情資引用列舉

- ✧ 美國國家漏洞數據庫
- ✧ 中國國家訊息安全漏洞庫
- ✧ Japan Vulnerability Notes
- ✧ CVE Common Vulnerabilities and Exposures
- ✧ OWASP Foundation
- ✧ MISP - Malware Information Sharing Platform, Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing
- ✧ Openphish
- ✧ PhishTank
- ✧ ClamAV
- ✧ 卡巴斯基訊息安全網站
- ✧ Google Safe Browsing®

ArmorX APT 操作介面

流量清洗

☐ 啟用 ☒ 不啟用

☐ 密碼保存
☐ 密碼輸入
☐ 密碼複讀

密碼連結 IP

登入 IP

☒ 啟用 ☐ 不啟用

☐ 詳細 每隔 分

☒ 清單表

序	時				日				月				周			
	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	○ 全部	
0	12	12	12	12	1	13	25	一月	一	星期一	星期一	星期一	星期一	星期一	星期一	
1	13	2	14	26	2	14	26	二月	二	星期二	星期二	星期二	星期二	星期二		
2	14	2	15	27	3	15	27	三月	三	星期三	星期三	星期三	星期三	星期三		
3	15	3	16	28	4	16	28	四月	四	星期四	星期四	星期四	星期四	星期四		
4	16	5	17	29	5	17	29	五月	五	星期五	星期五	星期五	星期五	星期五		
5	17	6	18	30	6	18	30	六月	六	星期六	星期六	星期六	星期六	星期六		
6	18	7	19	31	7	19	31	七月	七	星期日	星期日	星期日	星期日	星期日		
7	19	8	20		8	20		八月	八							
8	20	9	21		9	21		九月	九							
9	21	10	22		10	22		十月	十							
10	22	11	23		11	23		十一月	十一							
11	23	12	24		12	24		十二月	十二							

☒ 刪除件 ☐ 刪除件

程式行為

☒ 規則評分	☒ 防護型行為 (Antidebug Antivirus)	35	▼
	☒ CVE 漏洞掃描 (CVE Vulnerability)	25	▼
	☒ 0day 漏洞行為	25	▼
	☒ 私人漏洞揭露套件 (Exploit Kits)	35	▼
	☒ 隱藏位元組 (Packers Hidden)	15	▼
	☒ 文字指令碼 (Webshells)	25	▼
	☒ 惡意識別	50	▼
	☒ 惡意文件	100	▼
	☒ 惡意程式	100	▼
	☒ 系統登錄項目	100	▼
☒ 行為評分	☒ 惡意網址	35	▼
	☒ 行為分析	80	▼
	☒ 網路分析	50	▼

鑑識日誌

[illegible]

報表排程

報名課程

報名日期 ☒ 啟用 ☐ 不啟用

報名名額 名

☐ 詳情 每篇 篇 篇

☒ 詳情表

期	日	月	週
☐ 全部 ☒ 全部 ☐ 全部	☒ 全部 ☐ 全部 ☐ 全部	☒ 全部 ☐ 全部 ☐ 全部	☒ 全部 ☐ 全部 ☐ 全部
12	1 13 25	一月	星期一

☒ 今日
☐ 昨日
☐ 本週
☐ 上週
☐ 本月
☐ 上月
☐ 今年
☐ 去年

☐ 日
☐ 星
☐ 時
 小時

詳情時間 小時

收件卷

收件卷

主卷

來源點由

代碼代號

服務等價

收件卷

攔截統計

遠端名 Devs 拒絕管理 大量確認訊息 駭客名單 即時名單 攻擊統計

查詢範圍 ☒ 全部 ☐ 自 至

統計類別 ☒ 攻擊次數 ☐ IP 攻擊數

攻擊統計 - 攻擊總數

2020-12-19 ~ 2021-04-09

Category	Count	Percentage
hackers	2947515	83.02%
authen	481200	13.55%
reject	120286	3.39%
SYNC	1504	0.04%

釣魚行為

政策管理	政策運作模式	政策回收政策	政策評分
於局庫動作的政策 ☐ 啟用所有「的政策」 ☐ 啟用只有一條「的政策」			
參數運入選出 選擇標籤 選擇任何標籤 上一步 下一步			
選取 SpamTrap 政策			
啟用 SpamTrap 政策		SpamTrap 代號	
☒ 啟用自己		bkfkse1591	
☒ 啟用 ISP		bkfk/sf5952	
☒ 啟用內部網域		bkspnm1467	
☒ 啟用 ISP 惡名		bkdf/35820	
☒ 啟用內部網域		bkbddm1386	
☐ 僅於全部			

條件有前幾式條件的條件送前送前 選擇條件為：

- ☐ 連續傳信 (郵件: admin@myhost.mydomain.com.tw)
- ☐ 無連續傳信 (郵件: myhost.mydomain.com.tw)
- ☐ 造成垃圾傳信 (郵件: mydomain.com)
- ☐ 造成垃圾傳信 (郵件: mydomain.com)
- ☐ 造成垃圾傳信 (郵件: mydomain.com)
- ☐ 造成垃圾傳信 (郵件: mydomain.com)

1. 條件值置為 ISP 主機，但條件值置於不連續 ISP

2. 條件值置於連續網域並置，但值於一部主機置其真資訊

3. 條件值置 IP 地址中每部主機置 KKK IP

4. 條件值置 IP 地址中每部主機置 KKK 地址

5. 條件值置內部網域：符合其地址不連續型

6. 條件值置內部網域：符合其地址不連續型

7. 條件值置內部網域：符合其地址不連續型

8. 條件值置內部網域：符合其地址不連續型

9. 條件值置內部網域：符合其地址不連續型

10. 條件值置內部網域：符合其地址不連續型

11. 條件值置內部網域：符合其地址不連續型

12. 條件值置內部網域：符合其地址不連續型

13. 條件值置內部網域：符合其地址不連續型

14. 條件值置內部網域：符合其地址不連續型

15. 條件值置內部網域：符合其地址不連續型

16. 條件值置內部網域：符合其地址不連續型

17. 條件值置內部網域：符合其地址不連續型

18. 條件值置內部網域：符合其地址不連續型

19. 條件值置內部網域：符合其地址不連續型

20. 條件值置內部網域：符合其地址不連續型

21. 條件值置內部網域：符合其地址不連續型

22. 條件值置內部網域：符合其地址不連續型

23. 條件值置內部網域：符合其地址不連續型

24. 條件值置內部網域：符合其地址不連續型

25. 條件值置內部網域：符合其地址不連續型

26. 條件值置內部網域：符合其地址不連續型

27. 條件值置內部網域：符合其地址不連續型

28. 條件值置內部網域：符合其地址不連續型

29. 條件值置內部網域：符合其地址不連續型

30. 條件值置內部網域：符合其地址不連續型

31. 條件值置內部網域：符合其地址不連續型

32. 條件值置內部網域：符合其地址不連續型

33. 條件值置內部網域：符合其地址不連續型

34. 條件值置內部網域：符合其地址不連續型

35. 條件值置內部網域：符合其地址不連續型

36. 條件值置內部網域：符合其地址不連續型

37. 條件值置內部網域：符合其地址不連續型

38. 條件值置內部網域：符合其地址不連續型

39. 條件值置內部網域：符合其地址不連續型

40. 條件值置內部網域：符合其地址不連續型

41. 條件值置內部網域：符合其地址不連續型

42. 條件值置內部網域：符合其地址不連續型

43. 條件值置內部網域：符合其地址不連續型

44. 條件值置內部網域：符合其地址不連續型

45. 條件值置內部網域：符合其地址不連續型

46. 條件值置內部網域：符合其地址不連續型

47. 條件值置內部網域：符合其地址不連續型

48. 條件值置內部網域：符合其地址不連續型

49. 條件值置內部網域：符合其地址不連續型

50. 條件值置內部網域：符合其地址不連續型

51. 條件值置內部網域：符合其地址不連續型

52. 條件值置內部網域：符合其地址不連續型

53. 條件值置內部網域：符合其地址不連續型

54. 條件值置內部網域：符合其地址不連續型

55. 條件值置內部網域：符合其地址不連續型

56. 條件值置內部網域：符合其地址不連續型

57. 條件值置內部網域：符合其地址不連續型

58. 條件值置內部網域：符合其地址不連續型

59. 條件值置內部網域：符合其地址不連續型

60. 條件值置內部網域：符合其地址不連續型

61. 條件值置內部網域：符合其地址不連續型

62. 條件值置內部網域：符合其地址不連續型

63. 條件值置內部網域：符合其地址不連續型

64. 條件值置內部網域：符合其地址不連續型

65. 條件值置內部網域：符合其地址不連續型

66. 條件值置內部網域：符合其地址不連續型

67. 條件值置內部網域：符合其地址不連續型

68. 條件值置內部網域：符合其地址不連續型

69. 條件值置內部網域：符合其地址不連續型

70. 條件值置內部網域：符合其地址不連續型

71. 條件值置內部網域：符合其地址不連續型

72. 條件值置內部網域：符合其地址不連續型

73. 條件值置內部網域：符合其地址不連續型

74. 條件值置內部網域：符合其地址不連續型

75. 條件值置內部網域：符合其地址不連續型

76. 條件值置內部網域：符合其地址不連續型

77. 條件值置內部網域：符合其地址不連續型

78. 條件值置內部網域：符合其地址不連續型

79. 條件值置內部網域：符合其地址不連續型

80. 條件值置內部網域：符合其地址不連續型

81. 條件值置內部網域：符合其地址不連續型

82. 條件值置內部網域：符合其地址不連續型

83. 條件值置內部網域：符合其地址不連續型

84. 條件值置內部網域：符合其地址不連續型

85. 條件值置內部網域：符合其地址不連續型

86. 條件值置內部網域：符合其地址不連續型

87. 條件值置內部網域：符合其地址不連續型

88. 條件值置內部網域：符合其地址不連續型

89. 條件值置內部網域：符合其地址不連續型

90. 條件值置內部網域：符合其地址不連續型

91. 條件值置內部網域：符合其地址不連續型

92. 條件值置內部網域：符合其地址不連續型

93. 條件值置內部網域：符合其地址不連續型

94. 條件值置內部網域：符合其地址不連續型

95. 條件值置內部網域：符合其地址不連續型

96. 條件值置內部網域：符合其地址不連續型

97. 條件值置內部網域：符合其地址不連續型

98. 條件值置內部網域：符合其地址不連續型

99. 條件值置內部網域：符合其地址不連續型

100. 條件值置內部網域：符合其地址不連續型

鑑識報告

病毒沙箱掃描報告			
標題			
主機	test		
操作員	"Admin"<admin@armongt.com>		
收件員	"admin"<admin@armongt.com>		
日期	20210224		
訊息代號	1105mt68003141		
意見			
病毒分析			
標名	項目	分數	
virus.dll	惡意資料庫、反病毒行為 (Antidebug Antivm)、惡意遠端行為、malware、隱藏包殼 (Packers Hidden)	755	
權限		755	
掃描結果			
標名	virus.dll		
檔案符號	PE32 executable (DLL) (console) Intel 80386, for MS Windows		
檔案大小	92,672		
炸彈密碼 (Zip Bomb)	否		
惡意影響名	否		
附件加密	否		

資安事件 Line 通知

LINE 通知	更新通知	發送訊息
---------	------	------

LINE 通知	☒ 啟用 ☐ 不用	申請帳號
主旨	☒ 啟用 ☐ 不用	格式
本文	☒ 啟用 ☐ 不用	確定

新增	全部 查詢
----	---

每頁顯示: 50	50	第 1 頁 / 共 7 筆
----------	----	---------------

選取	帳號	帳號代碼	帳號名稱	動作
☐	數用	pZw2vzi3NLMN3r37gqsu3tU13CnfFZZzq2H4UJ	Alter_test	
☐	數用	H6tAq3j3BtCWj6a0tMnZ74589aSp5wepnbnr3zjFW	LOADER_MONITOR1	
☐	數用	9r8B0K7k7Vc0W04uNGnT6A1J3R6k6f9KAbaAm6wcl	DISK_MONITOR2	
☐	數用	aePw1ue0xVLCSQe0E4E7uW363zPy7d4qZsu8HJ8	UI 帳號名稱	
☐	數用	6vib356z0u0RRhcnzdWBDUQm68d3K3u5XNKGvV	Armor 通知	
☐	數用	7Gr3bLuP8r3c123H4D8f1In7FA4s4384jvu5pH	Daniel 通知	
☐	數用	ozcnrNhoM95FD3D94uXoN6z2BN86Hj6p5u6z5zY8	帳號名稱 tttt	
☐	帳號全部			

檢視項目 ☒ 啟用 ☐ 不用 ☐ 停用	確定
---	-----------------------------------