IBM Security

2020 年 IBM X-Force 威脅情報指數

IBM

IBM X-Force 事件回應和情報服務 (IRIS) 編製

目錄

摘要和關鍵趨勢 **4**

目標及初始感染媒介 **6**

針對營運技術 (OT) 基礎架構的攻擊呈爆炸性增長趨勢 6

遭洩露的記錄數量大幅增加 8

針對 IoT 裝置的攻擊目標涵蓋企業領域 9

在 2019 年的網路攻擊中，釣魚攻擊成為頭號初始存取媒介 11

惡意軟體趨勢 **13**

破壞性惡意軟體攻擊的數量大幅增加 13

勒索軟體和加密貨幣挖礦軟體在 2019 年猖獗肆虐 15

2019 年惡意軟體程式碼演變方面的頭號創新選手 16

銀行木馬與勒索軟體 - 一段越發危險的「聯姻」 19

垃圾郵件和釣魚攻擊的趨勢 **21**

2017 年的漏洞在 2019 年的垃圾郵件攻擊中繼續「發光發熱」 21

西方的垃圾郵件殭屍網路殃及全球 23

按地理區域劃分的垃圾郵件受害者 24

封鎖的惡意網域名稱凸顯了匿名化服務的普遍性 25

釣魚攻擊者仿冒技術公司、社群媒體 26

十大被仿冒品牌 28

目錄

最常受到攻擊的產業 **29**

金融與保險 30

零售 31

運輸 32

媒體與娛樂 33

專業服務 34

政府 35

教育 36

製造 37

能源 38

醫療保健 39

全球中心洞察 **40**

北美 41

亞洲 42

歐洲 43

中東 44

南美 45

為 2020 年的彈性應對做好準備 **46**

未來展望及關鍵要點 **47**

關於 X-Force **48**

摘要和關鍵趨勢

IBM Security 開發了各種智慧企業安全解決方案和服務，幫助您的企業增強抵禦未來網路安全威脅的能力。

為了讓安全專業人員瞭解最相關的威脅，IBM X-Force 會定期發佈有關新興威脅及攻擊者所用戰術、技術和程序 (TTP) 的部落格、白皮書、網路研討會和播客。

IBM Security 每年都會發佈 IBM X-Force 威脅情報指數報告，其中會總結我們的各個研究團隊在過去一年中發現的最突出威脅，向安全團隊提供相關資訊，以幫助他們更好地保護其組織。

本報告中提供的資料和洞察來自 IBM Security 托管的安全服務、事件回應服務、滲透測試活動及漏洞管理服務。

IBM X-Force 研究團隊分析了來自數億個受保護端點和伺服器的資料，以及來自非客戶資產（如垃圾郵件感應器和蜜網）的資料。IBM Security 研究團隊還在全球範圍內執行垃圾郵件陷阱，每天監控數以千萬計的垃圾郵件和釣魚攻擊，分析數十億個網頁和圖片，從中偵測攻擊活動、詐騙活動和品牌濫用，以更好地保護我們的客戶以及我們所處的互聯世界。

X-Force 事件回應和情報服務 (IRIS) 彙編了 IBM Security 在過去一年的軟體和安全服務分析結果，這些結果顯示 2019 年是舊威脅以新方式再度粉墨登場的一年。

- X-Force 的分析資料顯示，2019 年針對營運技術 (OT) 的攻擊事件數量增長了 2000%，這可能預示著：隨著我們邁入 2020 年，威脅實施者對攻擊工業系統的興趣「日漸濃厚」。

- 2019 年，共有超過 85 億條記錄遭到洩露，比 2018 年丟失的記錄數量高出 200% 以上。疏忽的內部人員是造成這種劇增的主要原因。2019 年，86% 的記錄由於伺服器設定錯誤（包括可公開存取的雲端儲存、不安全的雲端資料庫以及未適當予以安全保護的 rsync 備份或開放的網際網路連接網路區域儲存裝置）而遭到洩露。

- 這種惡意軟體威脅格局在 2019 年發生了變化，威脅實施者重新開始使用勒索軟體並建立了殭屍網路。2019 年，X-Force IRIS 回應了 5 大洲 12 個國家或地區的勒索軟體活動，這些活動涉及 13 個不同的產業。此外，破壞性惡意軟體活動的情況表明，這種潛在的災難性惡意軟體趨勢仍然是一個不斷上升的威脅。

- 在 X-Force IRIS 於 2019 年進行的互動中，排名前三位的初始感染媒介所占的比例非常接近，占比分別為：釣魚攻擊 (31%)、掃描與漏洞利用 (30%) 和憑證被盜 (29%)。最值得注意的是，釣魚攻擊在 2018 年占事件總數的近一半，而到 2019 年，其占比不足三分之一。相比之下，掃描與漏洞利用所占比例從 2018 年的 8% 增加到了 2019 年的近三分之一。

- -X-Force 對全球垃圾郵件活動分析後得出結論，垃圾電子郵件會繼續使用有限的漏洞，尤為值得關注的只有兩個 CVE：2017-0199 和 2017-11882。這兩個漏洞均為已修補的漏洞，在威脅實施者嘗試透過垃圾郵件活動利用的漏洞中占比近 90%。

- 儘管金融服務在 2019 年依然是受攻擊數量最多的產業，但從產業特定的攻擊目標也可以看出威脅實施者的優先攻擊目標有所變化，零售、媒體、教育和政府在全球最常受到攻擊的產業排名中均有所上升。

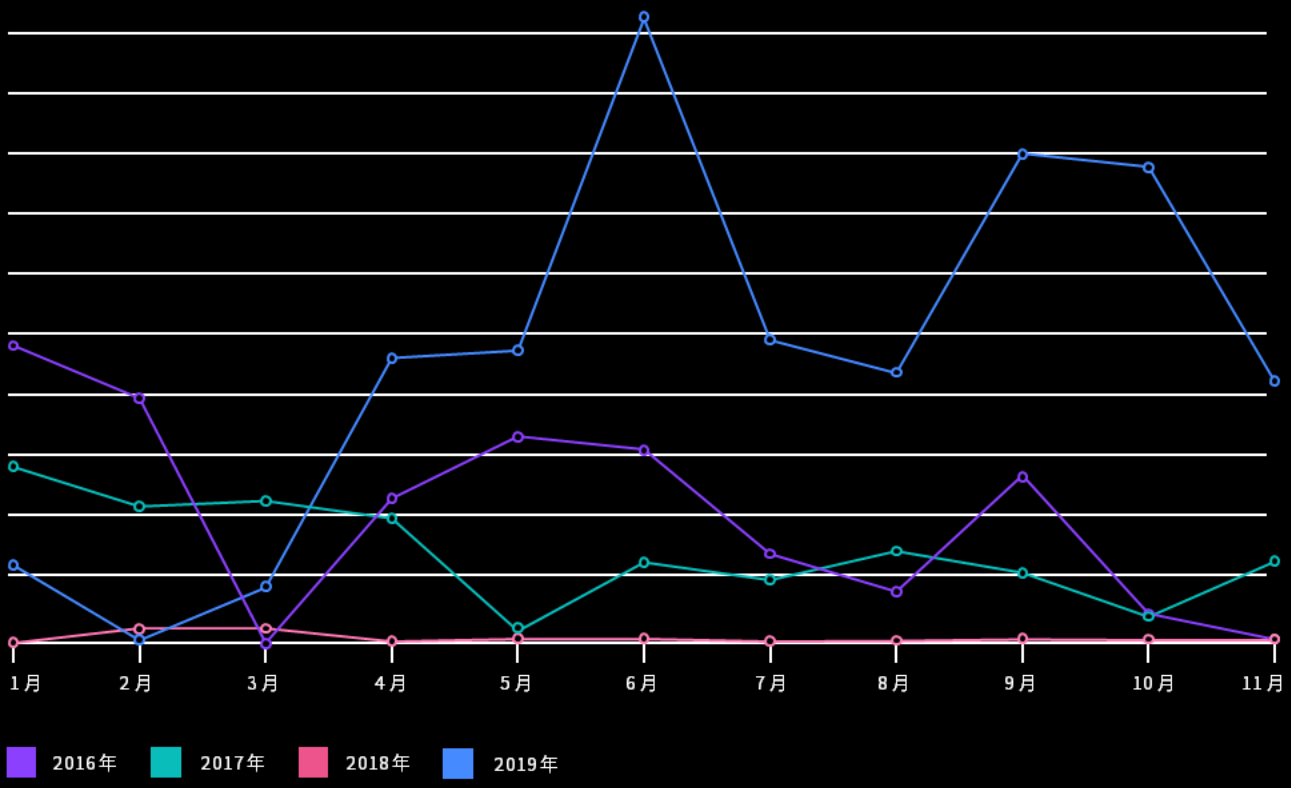
- 今年的 X-Force 威脅情報指數報告新增了全球中心洞察，旨在提供在全球範圍內監測到的趨勢資料。IBM Security 在今年繼續追蹤了針對所有地區的多種威脅實施者，而本報告重點介紹了針對每個地區的主要威脅實施者、從 2019 年開始監測到的攻擊以及在 2020 年可能需要重點關注網路安全的一些日期。

本年度報告的以下各節介紹了各方面的主要趨勢，並深入研究了形成 2019 年威脅格局背後的因素。

目標及初始感染媒介

圖 1：
營運技術 (OT) 攻擊趨勢

月 OT 攻擊量 - 對比 2016-2019 年的資料（來源：IBM X-Force）



針對營運技術 (OT) 基礎架構的攻擊呈爆炸性增長趨勢

IBM X-Force 分析資料表明，自 2018 年以來，威脅實施者針對工業控制系統 (ICS) 及類似營運技術 (OT) 資產的攻擊事件增加了 2000% 以上。實際上，2019 年針對 OT 資產的事件數量超過了過去三年監測到的活動數量總和。

大多數監測到的攻擊都是使用 SCADA 和 ICS 硬體組件內已知漏洞組合實施的攻擊，以及使用蠻力登入策略針對 ICS 目標進行的密碼噴霧攻擊。

據報導，一些針對 ICS 的攻擊活動與兩個已知的威脅實施者有關，而且與我們在遙測中監測到的攻擊時間軸激增不謀而合。Xenotime 組織和 Hive0016 (APT33) 發起了兩次特定活動，據報導，他們都擴大了對 ICS 目標的攻擊。

IT 基礎架構和 OT 之間的重疊，例如可程式化邏輯控制器 (PLC) 和 ICS，會繼續給 2019 年依賴此類混合基礎架構的組織帶來風險。

IT/OT 基礎架構的融合使得 IT 漏洞攻擊者可以將目標鎖定在控制實體資產的 OT 裝置，這就可能會大幅增加恢復成本。舉例來說，2019 年初，IBM X-Force IRIS 曾協助一家全球化製造公司應對資料洩露事件，一開始勒索軟體只是感染了 IT 系統，隨後逐漸蔓延至 OT 基礎架構，最終導致工廠營運停擺。這次攻擊不僅影響了該公司自身的營運，還在全球市場引發了連鎖反應。

2019 年為客戶提供的 X-Force IRIS 安全評估強調了 OT 系統的易受攻擊性，這些系統經常會使用遺留軟體和硬體。保留那些無法再修補且充斥著早已公之於眾的舊漏洞的生產系統，就意味著：即便 OT 系統並非面向網路，未經修補的 OT 系統也很容易成為犧牲品。在攻擊者找到第一個落腳點之後，如果發生橫向移動，就可以從網路內部存取這些系統，而且透過相對簡單的漏洞利用技巧即可實施破壞活動。

儘管圖 1 中顯示的 ICS 網路攻擊從 2019 年 10 月初以來呈現下滑趨勢，但 X-Force 預計，隨著威脅實施者不斷針對全球範圍內的工業網路發起新的活動，針對 OT/ICS 發起的攻擊在 2020 年會繼續增加。IBM X-Force 的漏洞資料庫顯示，2019 年新增了 200 多個與 ICS 相關的 CVE，針對 ICS 的威脅在 2020 年也會繼續保持增長態勢。

X-Force 預計，隨著世界各地的威脅實施者對工業網路不斷發起新的活動，針對 ICS 發起的攻擊在 2020 年會繼續保持增長勢頭。

遭洩露的記錄數量大幅增加

洩露記錄的數量在 2019 年大幅飆升，外洩記錄數已超過 85 億條 - 相比 2018 年，年成長率增長三倍以上。造成這種大幅飆升的「罪魁禍首」，是由於錯誤配置導致的記錄洩露年成長率增長了近十倍。這些記錄占到了 2019 年資料洩露數量的 86%。這與我們 2018 年報告的數字有著很大不同，當時我們監測到，因為錯誤配置而洩露的記錄數量比 2017 年減少了 52%，這些記錄數量尚未占到總記錄的一半。

值得注意的是，2019 年錯誤配置事件的數量實際上比上一年減少了 14%。這一事實反映了一個問題：在 2019 年，對於發生的錯誤配置事件，受影響記錄的數量有顯著增加。近四分之三的洩露中，有超過一億條遭洩露記錄是由於錯誤配置事件所致。在專業服務業發生的兩起錯誤配置事件中，每起事件洩露的記錄數量都高達數十億條。

各產業丟失記錄的數量大幅增加，凸顯了資料洩露不斷攀升的風險，即便那些通常不會視作主要目標的產業內的組織也是如此。

2019 年洩露的記錄數量

85 億條

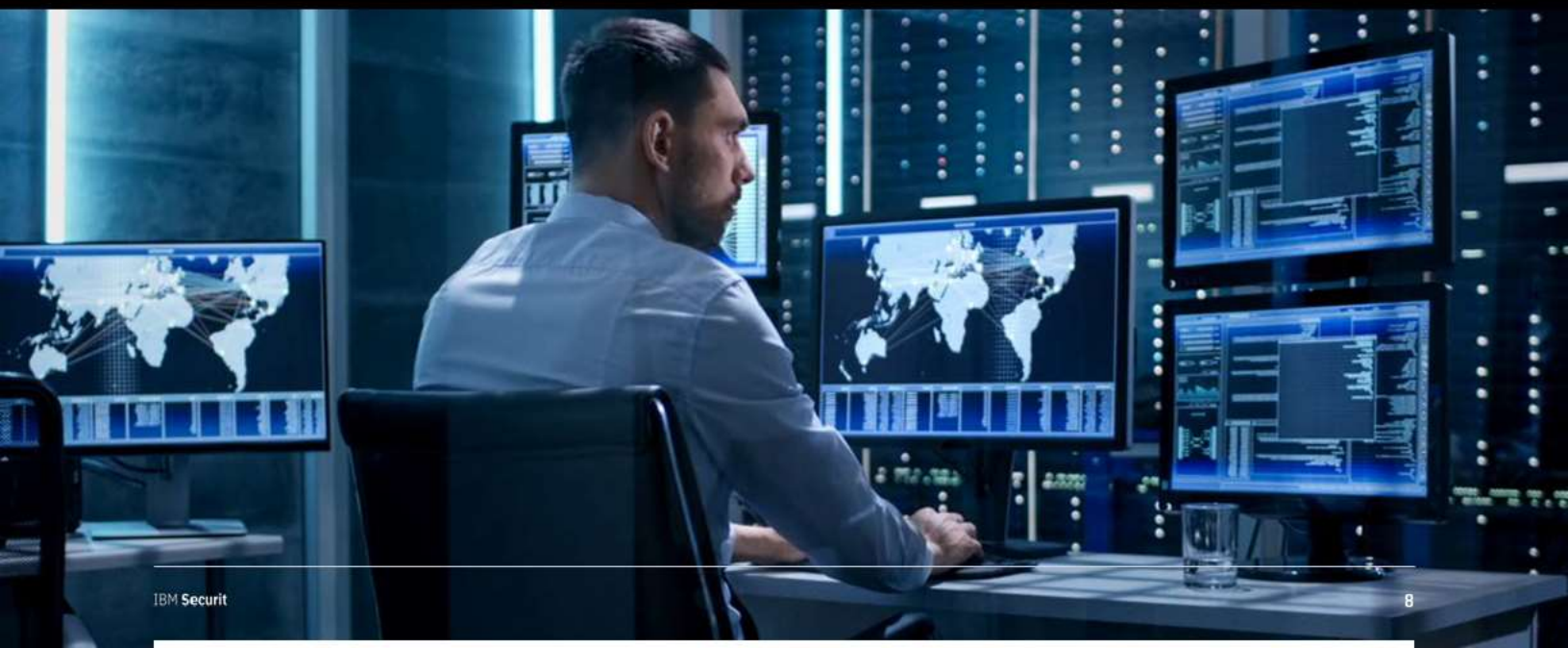
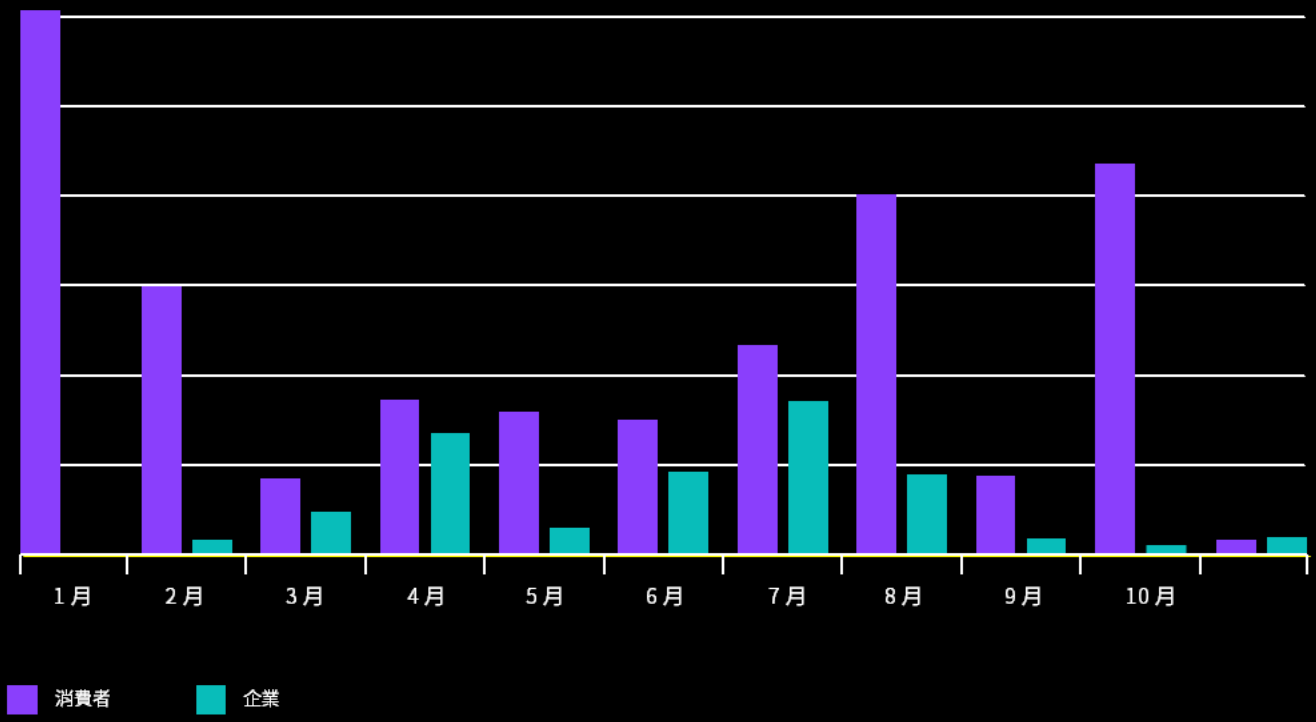


圖 2：
針對消費者與企業 IoT 的攻擊

2019 年消費者與企業 IoT 每月遭受的攻擊量（來源：IBM X-Force）



針對 IoT 裝置的攻擊目標涵蓋企業領域

2020 年，接入網際網路的裝置將超過 380 億台，物聯網 (IoT) 威脅格局已逐漸明朗，已成為影響消費者和企業級營運的威脅媒介之一，它們通常會使用相對簡單的惡意軟體和一般使用指令碼編寫的自動攻擊。

在用於入侵 IoT 裝置的惡意程式碼的範圍內，IBM X-Force 研究團隊在 2019 年追蹤了多次 Mirai 惡意軟體活動，這些活動都有一個明顯的趨勢：它們將攻擊的矛頭從消費性電子產品轉向了企業級硬體，這是我們在 2018 年並未監測到的活動。駭客可以將聯網的受感染裝置作為中轉站，以伺機在組織內「安營紮寨」。

Mirai 是一款「作惡多端」的 IoT 惡意軟體，從 2016 年以來，駭客們便一直利用這款軟體製造大規模破壞，它會感染大量物聯網裝置並將它們用在分佈式拒絕服務 (DDoS) 攻擊中。透過分析 2019 年的活動，我們發現，自 2018 年以來，使用 Mirai 惡意軟體的戰術、技術和程序 (TTP) 發生了顯著的變化，2019 年，它們的攻擊目標除了消費性電子產品之外，還增加了企業硬體。

深入研究 2019 年對 IoT 裝置造成影響的攻擊之後，我們發現命令注入 (CMDi) 攻擊十分猖獗，這些攻擊中包含用於下載惡意有效負載的指令，以攻擊不同類型的 IoT 裝置。大部分此類注入攻擊都是透過指令碼自動發起，指令碼會掃描並試圖大規模感染裝置。如果作為攻擊目標的 IoT 裝置容易受到此類注入攻擊，就會下載並執行有效負載，而且會將裝置迅速拉入龐大的 IoT 殭屍網路。這些攻擊之所以能夠得手，一個最常見的「幕後推手」就是 IoT 裝置使用了較弱或預設的密碼，哪怕是一次微不足道的字典式攻擊也能輕易猜出密碼。

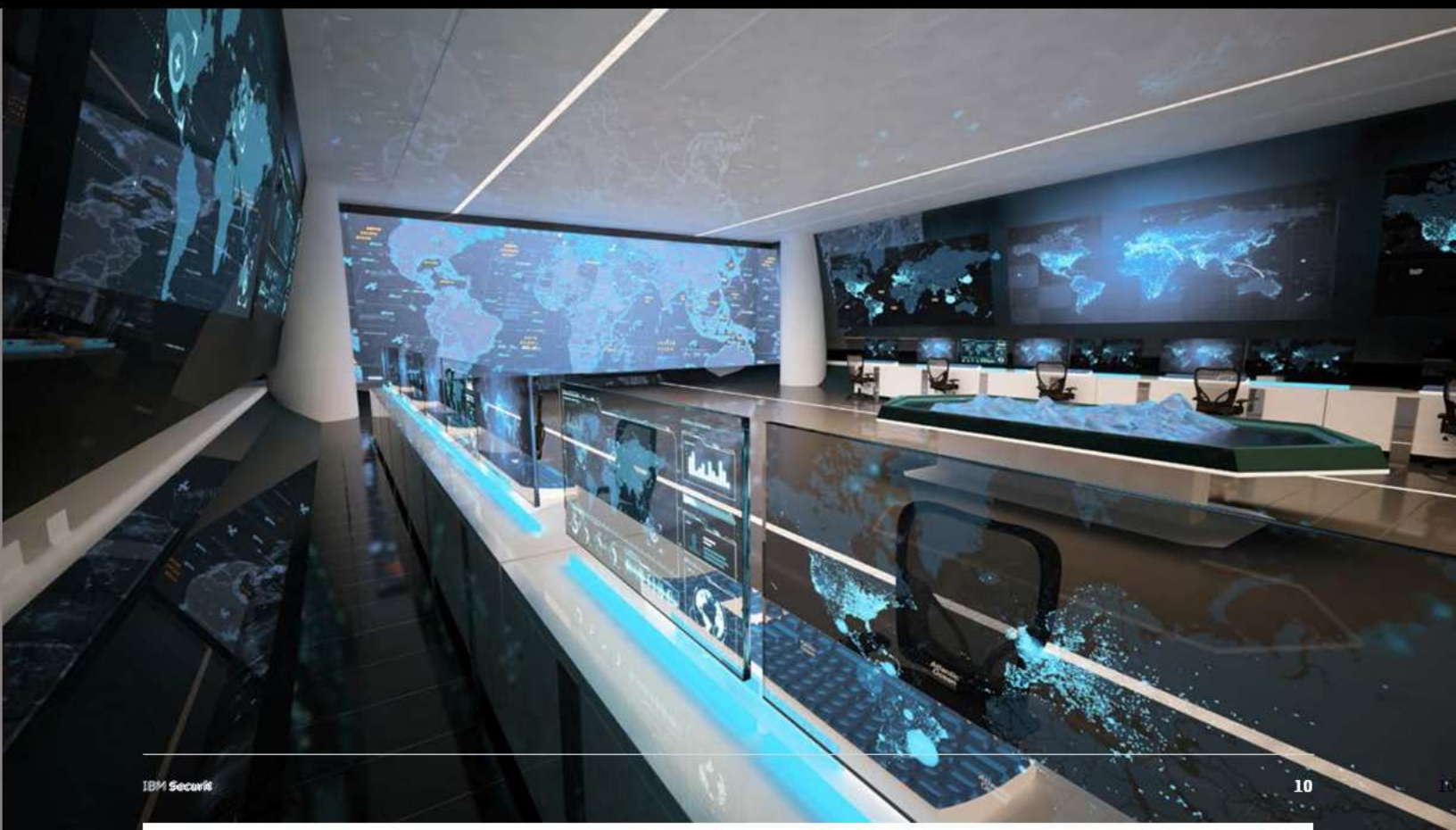
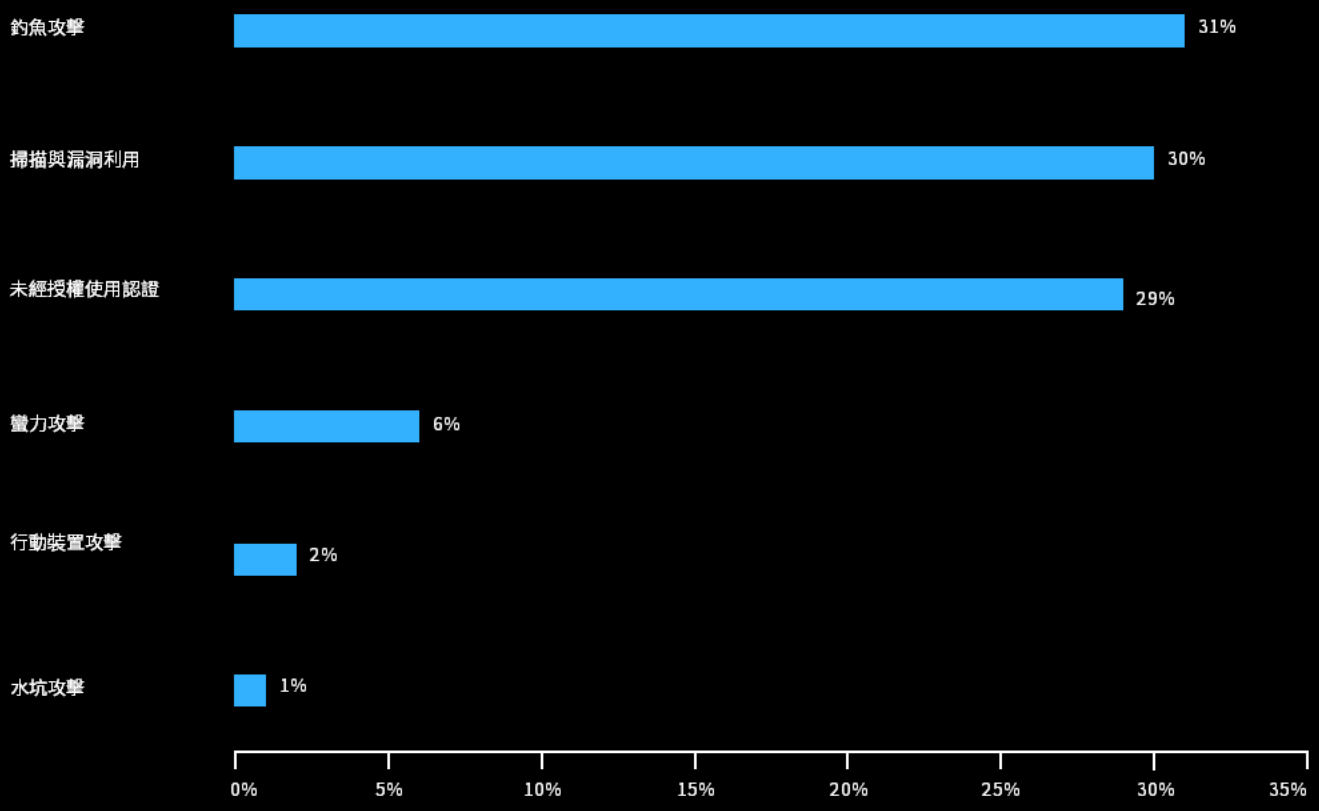


圖 3：
主要的初始存取媒介

2019 年最主要的 6 種初始攻擊媒介的細分，以百分比顯示的 6 種存取媒介（來源：IBM X-Force）

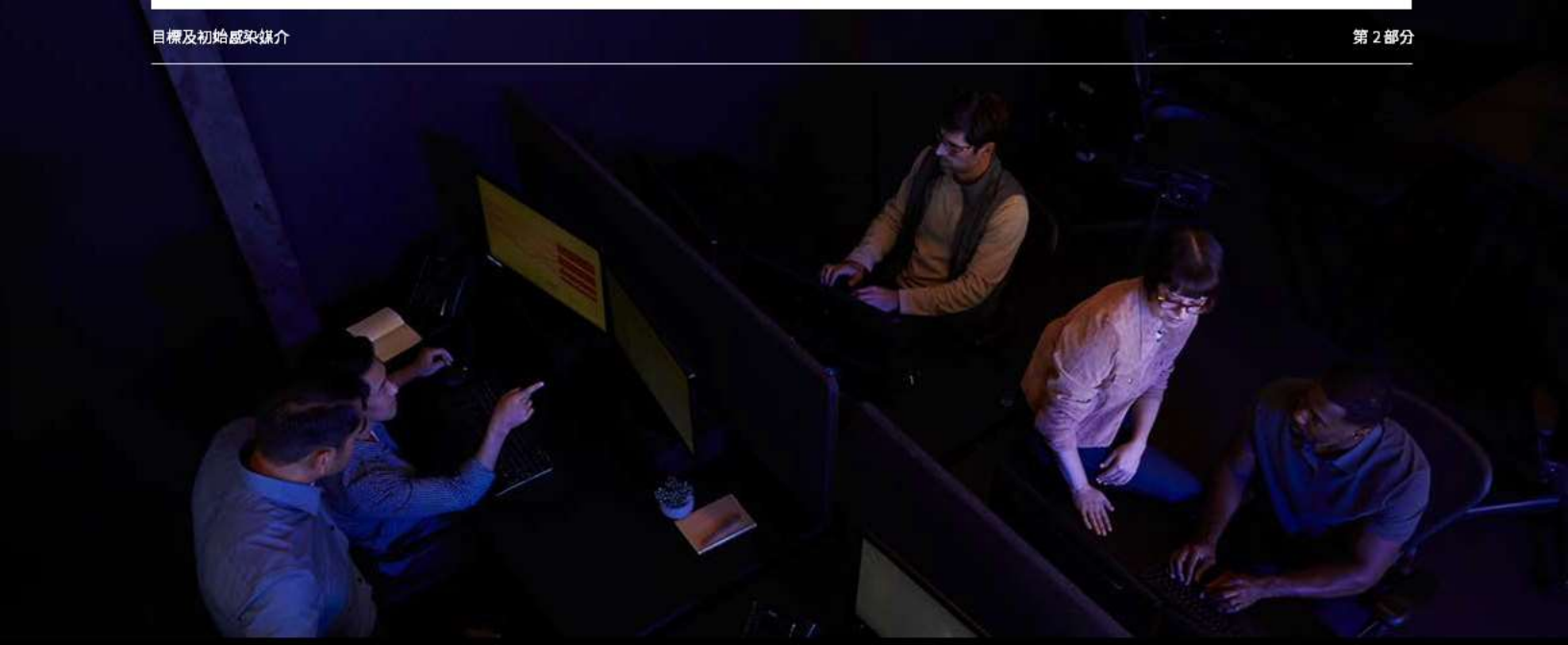


在 2019 年的網路攻擊中，釣魚攻擊成為頭號初始存取媒介

IBM X-Force IRIS 擁有廣泛的事件回應能力，能夠對攻擊方法和動機提出寶貴的洞察。

2019 年，釣魚攻擊是初始存取最常用的媒介，占比為 31%，但與 2018 年相比有所下降，當時釣魚攻擊占到了總數量的近一半。[1]

1 2019 年 X-Force 威脅情報指數報告顯示，在 X-Force IRIS 分析的攻擊中，有近三分之一 (29%) 的破壞活動是透過釣魚電子郵件發起的。此後已對該數字進行了調整，因為幾起事件在揭露之後有更多證據浮出水面，使這一比例在 2018 年增加至 44%。



最值得注意的是，2019 年，攻擊者愈來愈多地開始掃描目標環境，以發現可以利用的漏洞，事件回應人員發現，有 30% 的事件使用了這一伎倆，而在上一年，此類攻擊僅占總事件的 8%。

威脅實施者可以選擇的掃描和利用的對象有很多，IBM X-Force 追蹤了 150,000 多個已公開揭露的漏洞。一些老奸巨猾的對手會開發零日漏洞，透過依賴比此類零日漏洞更頻繁發生的已知漏洞，對手不需動用一兵一卒來擬定新的 TTP 即可初步站穩腳跟，利用他們最有殺傷力的武器來侵入防禦能力最強的網路。此外，攻擊者會寄希望於那些沒有更新其修補程式的組織，儘管有些漏洞的修補程式在很久前便已推出。舉例來說，自發生首例 WannaCry 感染並廣泛推廣修補程式 (MS17-010) 之後的兩年多內，WannaCry 感染現象仍然層出不窮。

威脅實施者使用之前獲取的憑證來存取目標組織，即使用被盜憑證實施的攻擊以 29% 的比例占到了近三分之一。這些憑證通常是從第三方網站竊取，或是透過向目標組織發起的釣魚攻擊而獲得。威脅實施者可以使用被盜憑證混進合法流量中，要發現它們的蹤跡就變得難上加難。

蠻力攻擊與上一年相比有所下降，以 6% 的占比在所有事件中排名第四，緊隨其後的是 BYOD 裝置 (2%)，它是進入目標組織的初始存取點。

X-Force 研究人員發現，威脅實施者的活動在 2019 年 6 月份和 7 月份有顯著的增長，這段時期的事件數量超過了 2019 年全年的總數。儘管活動數量突然暴增的原因不得而知，垃圾郵件在夏季也似乎更加活躍，其數量在 2019 年 8 月達到峰值。

原因可能是威脅實施者變得更加招人耳目，更容易被發現，又或者是因為威脅實施者戰略或工具發生改變而產生了大量活動。但出現短暫的活動峰值不太可能是因為有新的威脅實施者進入市場，因為若出現新的威脅實施者，勢必會讓活動持續增加，而不是這般曇花一現。

惡意軟體趨勢

破壞性惡意軟體攻擊的數量大幅增加

IBM X-Force IRIS 調查發現，2019 年，破壞性惡意軟體攻擊變得更加頻繁，並且無論是攻擊的地理範圍還是規模都有所增加。

破壞性惡意軟體是網路犯罪分子和民族國家威脅實施者常用的伎倆，它能夠使受影響的系統無法運作，並讓重建變得困難重重。大多數破壞性惡意軟體變體都會透過刪除或覆寫對作業系統執行能力而言至關重要的檔案，來達到破壞的目的。在少數情況下，破壞性惡意軟體可能會向工業裝置傳送量身定制的訊息以引發故障。在我們對破壞性惡意軟體的定義中還有一類勒索軟體，它能夠清除機器上的資料或對機器上的資料進行不可逆的加密。

2018 年下半年與 2019 年下半年，2019 X-Force IRIS 處理了相同數量的破壞性攻擊，不難看出，這種潛在的災難性惡意軟體會繼續讓組織面臨風險。

從歷史上看，破壞性攻擊通常來自民族國家對手。但我們監測到這麼一種趨勢：愈來愈多受經濟利益驅動的勒索軟體會在攻擊中使用破壞性元素，以變體 LockerGoga 和 MegaCortex 為例，它們在 2018 年底和 2019 年初首次發動了破壞性攻擊。

破壞性攻擊造成的損失平均在 2.39 億美元左右，是資料洩露平均成本的 60 倍以上。

2019 年底，X-Force IRIS 發現了一種名為 ZeroCleare 的新型破壞性惡意軟體。這款刪除式惡意軟體的攻擊目標是中東的金融業，IBM 認定它來自隸屬於伊朗的 APT 集團 ITG13[2]（也被稱為 APT34/OilRig）。

X-Force IRIS 預計，破壞性惡意軟體攻擊會讓公司付出慘重的代價，大型跨國公司在每起事件後支付的平均成本高達 2.39 億美元。此成本估算是 2019 年資料洩露平均成本的 60 倍以上。與專門竊取或暴露資料的資料洩露的不同之處在於，破壞性攻擊通常會讓受害組織四分之三甚至更多的裝置毀於一旦。

2 ITG 是 IBM Threat Group 的縮寫，我們在「最常受到攻擊的產業」中會進一步探討這一術語。X-Force 使用 ITG 名稱，並在 ITG 名稱後面的括弧中指明威脅團夥的備用名稱。

勒索軟體和加密貨幣挖礦軟體在 2019 年猖獗肆虐

惡意軟體變體以及使用惡意軟體發動的攻擊數量在一年內起起伏伏，但是儘管如此，對那些不容忽視的威脅類型的瞭解會幫助組織更好地管理風險。

2019 年上半年，我們監測到的攻擊中約有 19% 與勒索軟體事件有關，而 2018 年下半年這一比例僅為 10%。2019 年第 4 季度，勒索軟體活動與上一年第 4 季度相比增加了 67%。2019 年，X-Force IRIS 回應了 5 大洲 12 個國家或地區的勒索軟體活動，這些活動涉及 13 個不同的產業。

這種激增可能是由於 2019 年威脅實施者以及針對不同組織發起的活動數量不斷增長導致的。值得注意的是，受到勒索軟體攻擊的除了市政和公共機構之外，還有地方政府機構和醫療保健提供者。對這些組織發起的攻擊常常會令他們措手不及，只得支付贖金，並且在某些情況下，因為會威脅到公共安全和生命，他們還要承受巨大的壓力從攻擊中迅速恢復。

X-Force 資料顯示，在勒索軟體攻擊活動中，2019 年的頭號攻擊媒介是利用 Windows SMB 協定中的漏洞透過網路進行傳播。這一伎倆曾在 WannaCry 攻擊中用過，占到了已監測到的攻擊嘗試的 80% 以上。

與 2018 年第四季度相比，2019 年第四季度的勒索軟體活動增加了 67%。

圖 4：
多階段勒索軟體感染

分多階段入侵的勒索軟體攻擊（來源：IBM X-Force）

SMB 協定帶有安全漏洞，針對該協定的攻擊可以自動發起，這使它成為了威脅實施者的一種低成本攻擊選項，且更易於擴展攻擊範圍，可以在一次攻擊中影響儘可能多的系統。

威脅實施者還經常使用 Emotet 和 TrickBot 等常見的商用下載器，在目標系統上執行勒索軟體。這種手段經常會利用 PowerShell 下載惡意軟體，並利用 PSExec 或 Windows Management Instrumentation (WMI) 等本機功能進行傳播，進而進一步加大了偵測難度。

攻擊者會分多個階段來感染使用者，而不是利用勒索軟體直接命中目標，這樣一來，攻擊者能夠更好地掌控攻擊，逃避控制措施和偵測，並埋下勒索軟體操作的種子，感染儘可能多的裝置，從而迫使受害者就範，甘願支付贖金。這種耐心和籌謀帶來了豐厚的回報：短短五個月內，Ryuk 攻擊就為他們的犯罪集團積斂了 370 多萬美元的不義之財。在另一個實例中，Ryuk 營運商對美國養老院發動攻擊並索要 1400 萬美元的贖金。

勒索軟體並不是 2019 年唯一一款異軍突起的惡意軟體。加密貨幣挖礦程式碼是 2019 年另一款格外猖獗的惡意軟體。

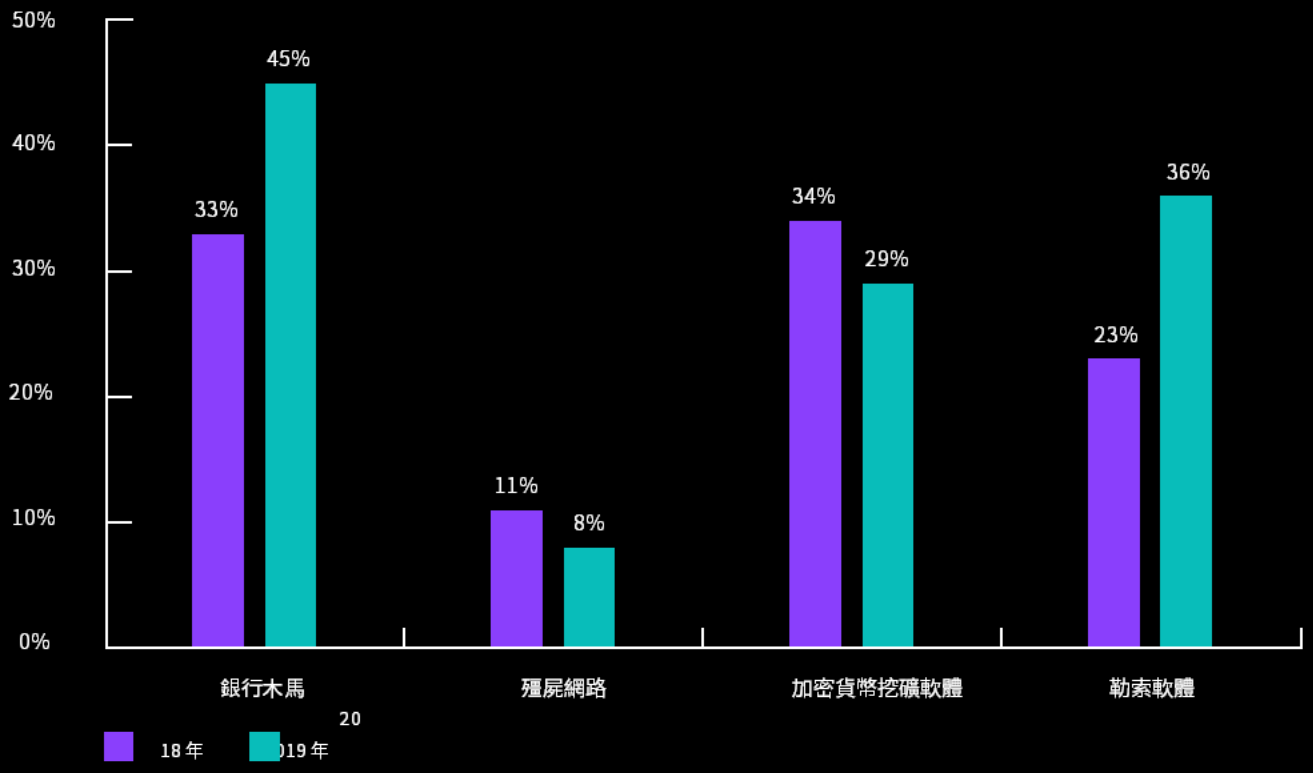
據 X-Force 遙測，加密挖礦活動在 2019 年中期飆升至前所未有的水準，6 月份的活動數量幾乎已經超過了全年所有的其他加密挖礦活動的總和。

儘管惡意軟體趨勢隨著殭屍網路營運商的動機和資源起起伏伏，但是這種激增卻可能與 Monero 的價值飆升三倍有關 - Monero 是惡意軟體礦工經常使用的一種加密貨幣。

圖 5：

惡意軟體遺傳程式碼創新

按類別劃分的新（之前未監測到）程式碼百分比，2018-2019 年（來源：Intezer）



2019 年惡意軟體程式碼演變方面的頭號創新選手

透過借鑑 X-Force 之前在偵測新惡意軟體變體方面的協作，Intezer 利用其遺傳惡意軟體分析技術揭示了所有軟體程式碼的遺傳來源，從中發現程式碼相似性和程式碼復用，以測量惡意軟體的「升級換代」。這種測量與威脅實施者投資開發新程式碼的力度相當，從中可以看出對手也在積極擴大其威脅能力並竭力逃避偵測。

Intezer 提供的資料顯示，2019 年，威脅實施者主要側重於開發和升級銀行木馬和勒索軟體的程式碼庫，同時還在不遺餘力地修改和製造加密挖礦惡意軟體毒株。

報告的這一部分由 IBM X-Force 和 Intezer 研究人員合作完成。Intezer 針對惡意軟體的二進位程式碼執行了遺傳分析。

2019 年，銀行木馬在新程式碼中所占比例最高 (45%)，勒索軟體緊隨其後 (36%)。就過去經驗看來，IBM 發現威脅實施者對那些可以有效攻擊企業使用者的惡意軟體類型保持著濃厚的興趣，而且不斷對其進行投資，這表明這些惡意軟體家族可能會在 2020 年將企業作為攻擊目標。如果他們不持續改進，銀行木馬和勒索軟體營運商將會陷入絕境，因為惡意軟體會更快地被偵測出來並降低攻擊的長期投資回報。

2019 年，威脅實施者集中精力開發和升級銀行木馬和勒索軟體的程式碼庫。

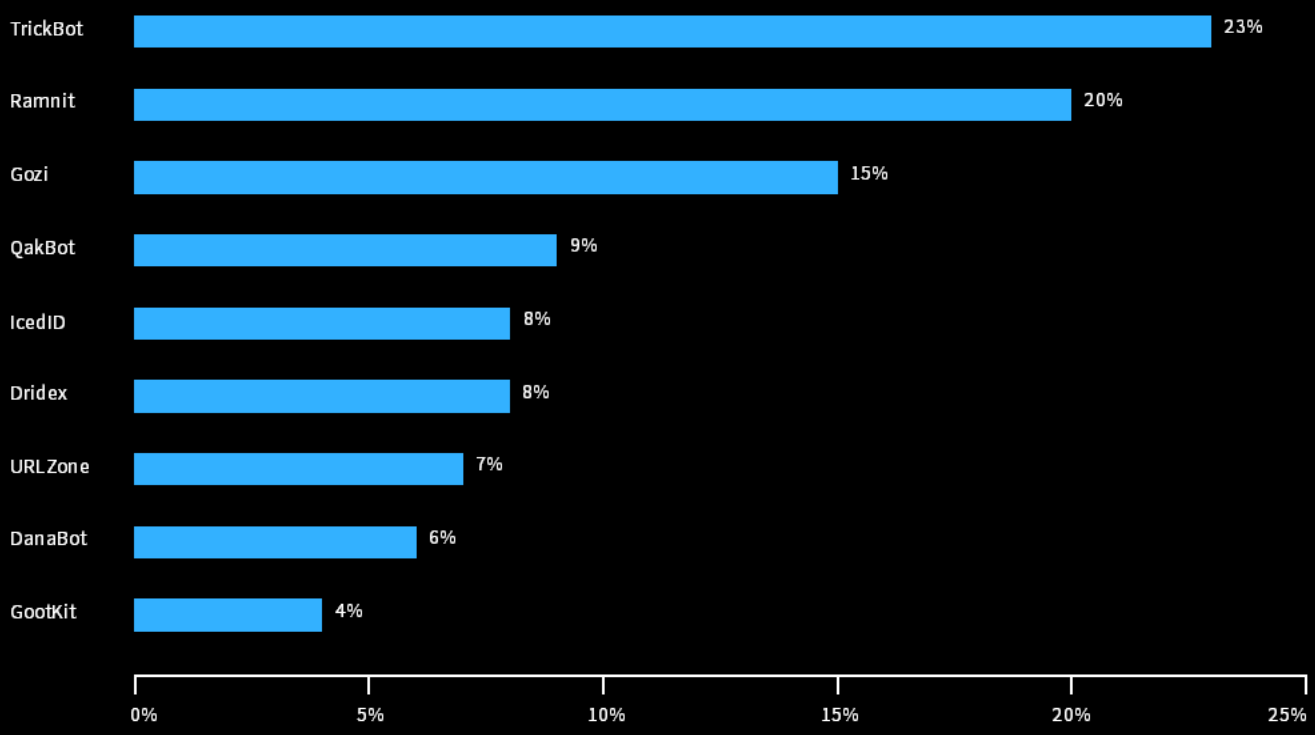
2019 年，加密貨幣挖礦軟體的創新能力有所下降，但挖礦活動量仍居高不下，這表明威脅實施者會繼續開發新版本的加密貨幣挖礦軟體，但也更加依賴之前的程式碼。根據 IBM 的經驗，這些簡單的惡意軟體程式碼往往會依賴其他一些無惡意的「前輩」，例如 XMRig，他們對 XMRig 進行修改之後便能以非法方式將財富收入囊中。不過，他們也會出於不同的目的編寫新的挖礦程式，例如對 IoT 裝置收割財富，或者在另一個極端 - 對感染伺服器收割財富，伺服器的 CPU 功耗要高於小型裝置和單個 PC。

相比之下，一般的殭屍網路惡意軟體 (11%) 每年的程式碼創新較少，這表明威脅實施者減少了在修改其功能方面的投資。IBM 發現這些類型的程式碼是透過垃圾郵件或惡意廣告推送給使用者的。一般殭屍網路惡意軟體的主要作用是在受感染的裝置上站穩腳跟，但它們的功能仍然極其有限，這也就解釋了它們的程式碼進化等級為何一直較低。

2020 年，從這些程式碼創新趨勢中可以看出某些需要更多投入來識別和遏制的惡意軟體。

圖 6：
主要的銀行木馬家族

2019 年主要銀行木馬家族細分，以百分比顯示九大木馬家族（來源：IBM X-Force）



銀行木馬與勒索軟體 - 一段越發危險的「聯姻」

十多年前，隨著宙斯木馬之類的惡意軟體的興起，金融惡意軟體成為了一個主流問題，宙斯木馬是當時的網路犯罪領域第一個普遍可用的商業銀行木馬。回顧 2019 年金融犯罪情勢，從中可以看出主要銀行木馬犯罪團夥的明顯趨勢：這些惡意軟體殭屍網路愈來愈多地被用於敲開攻擊目標的大門，然後實施高回報的勒索軟體攻擊。

2019 年該類別中最活躍的特洛伊木馬家族的圖表與我們在 2018 年度綜覽中產生的圖表非常相似。TrickBot、Gozi 和 Ramnit 占據了前三名的位置。這些特洛伊木馬由有組織的團夥負責營運，這些團夥為其他網路犯罪參與者提供不同的商業模式，例如殭屍網路租用服務計畫以及透過淪陷的資產進行傳播。

到目前為止，營運 TrickBot 的團夥是 2019 年網路犯罪領域最活躍的犯罪軟體團夥。這種活動表現在多個不同的方面：

- 程式碼更新和修復的頻率（程式碼、版本和功能演變）

- 入侵活動的頻率和規模

- 攻擊活動的頻率和數量

2019 年發起高風險勒索軟體攻擊並成為頭條新聞的團夥，正是 2015 年在網路犯罪領域引入高風險電信欺詐活動的始作俑者。在某種意義上來說，總體戰略基本一樣，只對具體策略做出了一些改動：瞄準企業牟取更豐厚的回報。

演變成勒索軟體的主要銀行木馬示例：

Dridex
之前是將 LokiBot 傳播到使用者裝置上，現在是在企業網路上部署 BitPaymer/DopplePaymer。

GootKit
在企業網路上部署 LockerGoga 的嫌疑分子。LockerGoga 在 2019 年初出現，已經成為向企業發起精準攻擊的中堅力量。

QakBot
在企業網路上部署 MegaCortex。

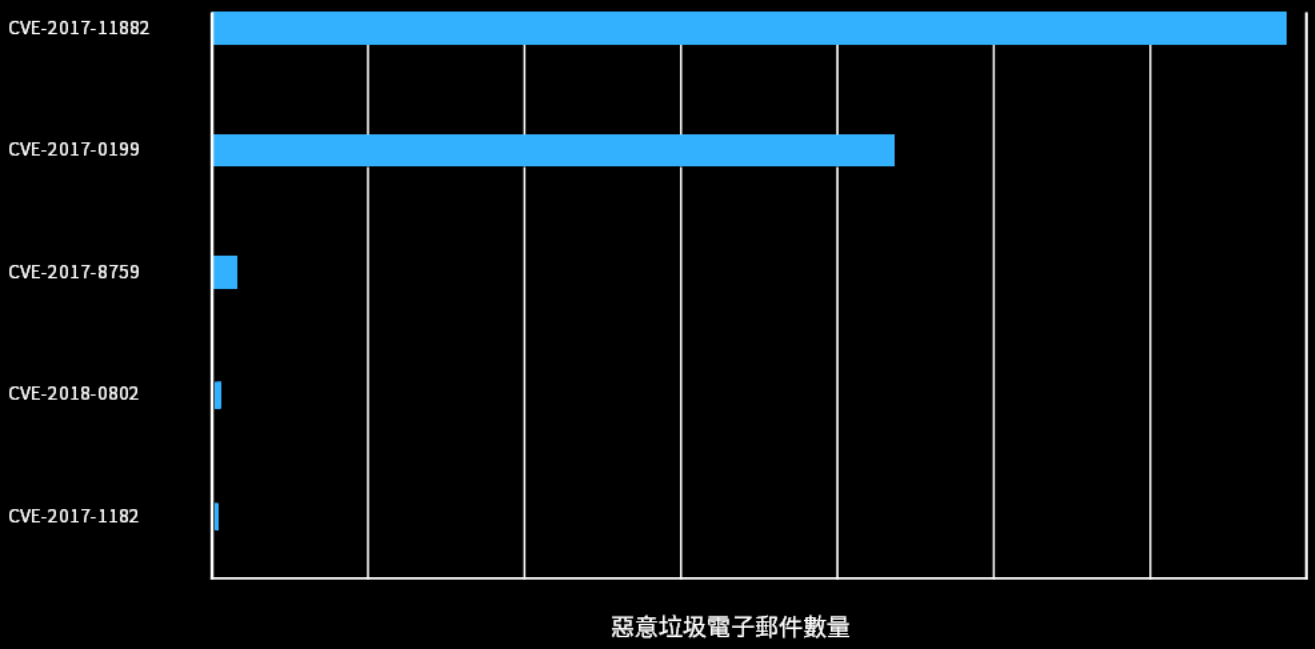
TrickBot
在企業網路上部署 Ryuk。

此外，2019 年底的報告顯示，一直以來專門大規模竊取支付卡資料的 ITG08 (FIN6) 也在努力讓自己的 TTP 實現多樣化發展。它現在的工作重心是要在企業網路上部署勒索軟體。收集、銷售或使用竊取的卡資料，需要投入大量時間和精力才能變現，而勒索軟體攻擊卻能不費吹灰之力便將數百萬美元收入囊中，這一巨大的利潤誘使更多犯罪團夥去使用勒索軟體並走上網路敲詐勒索的道路。

垃圾郵件和釣魚攻擊的趨勢

圖 7：
惡意垃圾郵件中利用的主要漏洞

2019 年惡意垃圾郵件附件中利用的主要漏洞細分，按數量劃分（來源：IBM X-Force）



2017 年的漏洞在 2019 年的垃圾郵件攻擊中繼續「發光發熱」

IBM X-Force 每天都會執行世界各地的垃圾郵件陷阱，並監控數以千萬計的垃圾資訊和釣魚攻擊電子郵件。我們的團隊和技術人員會分析數十億計的網頁和圖片，以偵測詐欺活動和品牌濫用。

X-Force 對全球垃圾郵件活動分析後得出結論，垃圾電子郵件會繼續使用有限的漏洞，尤為值得關注的只有兩個 CVE：2017-0199 和 2017-11882。這兩個漏洞均為已修補的漏洞，在威脅實施者嘗試透過垃圾郵件活動利用的漏洞中占比近 90%。這些 CVE 都會影響 Microsoft Word，並且除了開啟一份設置了陷阱的文件之外，根本無需使用者操作。

我們的事件資料顯示，2019 年攻擊者利用這兩個漏洞的頻率比任何其他 Microsoft Word 遠端程式碼執行漏洞的使用頻率高出近 5 倍。

儘管這兩個漏洞是大量垃圾電子郵件的常客，但並不能因此說明它們在攻擊使用者方面有多麼成功。也就是說，垃圾郵件常常是一個數字遊戲；只要數量足夠，即便是一次偶然的成功也能為威脅實施者帶來收益。因為許多使用者甚至是組織都不能做到及時修復問題，因此攻擊者仍可使用原來的漏洞對裝置發起攻擊。

原來的漏洞長盛不衰的原因有很多，例如可以輕鬆植入、可以使用免費的文件產生器、具有持續的效力或者是因為它們的多功能性，可以投放各種惡意的有效負載等等。

原有漏洞的持續使用凸顯了惡意活動的長尾效應，還可以看出，在揭露和修補程式發佈數年後仍可利用重大漏洞攻擊使用者。

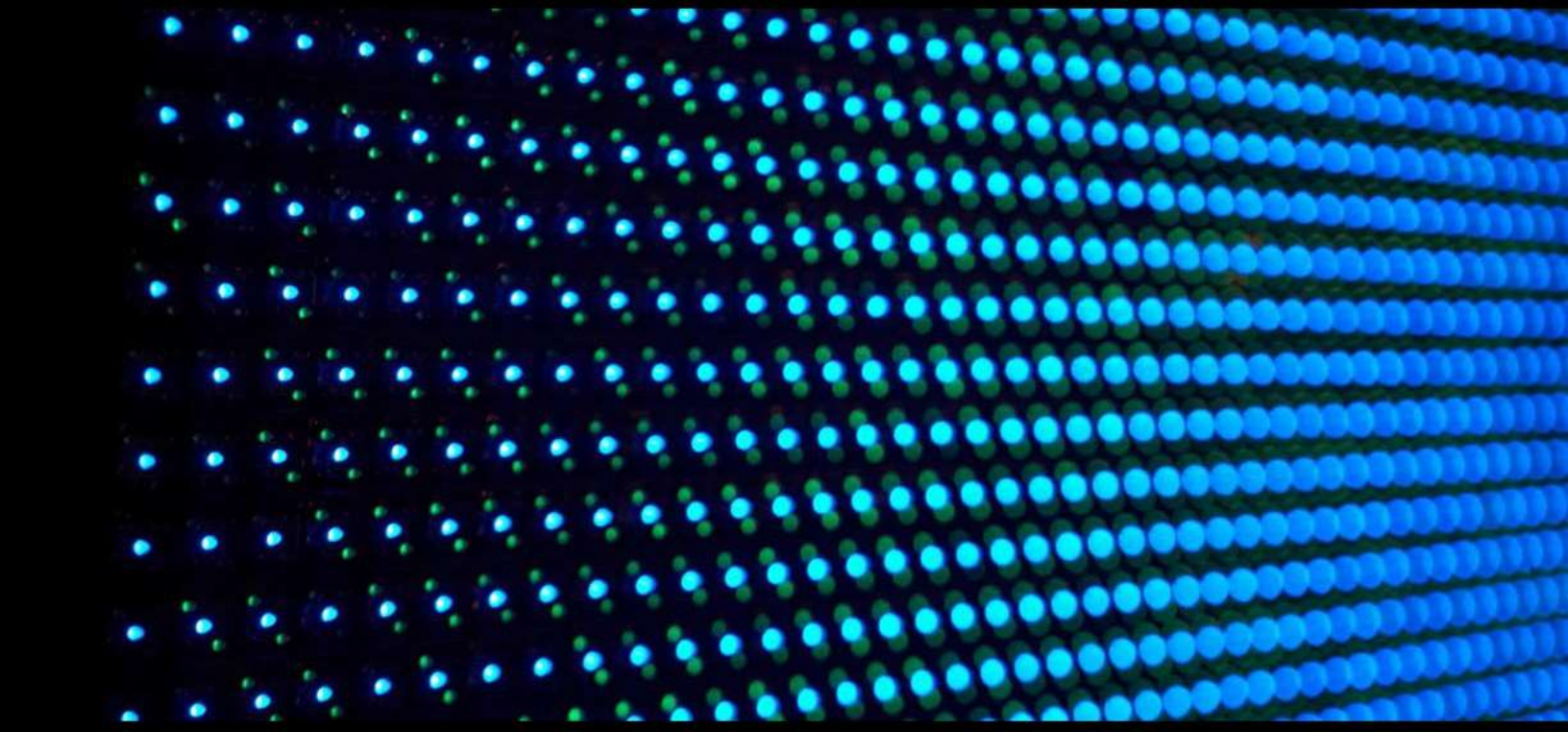
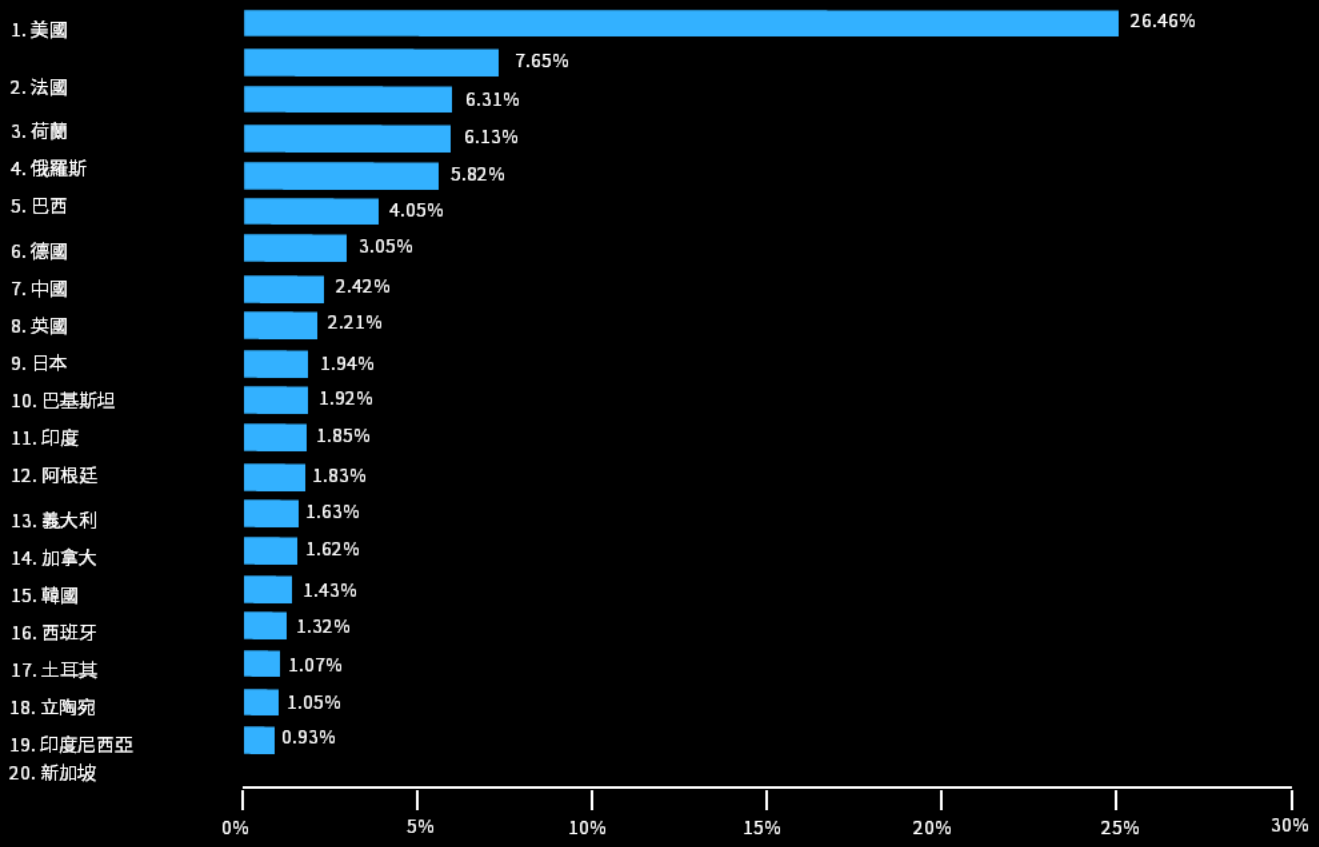


圖 8：

垃圾郵件 C2 托管排名前 20 位的國家或地區

2019 年按全球垃圾郵件命令與控制 (C2) 伺服器份額排名前 20 位的國家或地區。（來源：IBM X-Force）



西方的垃圾郵件殭屍網路殃及全球

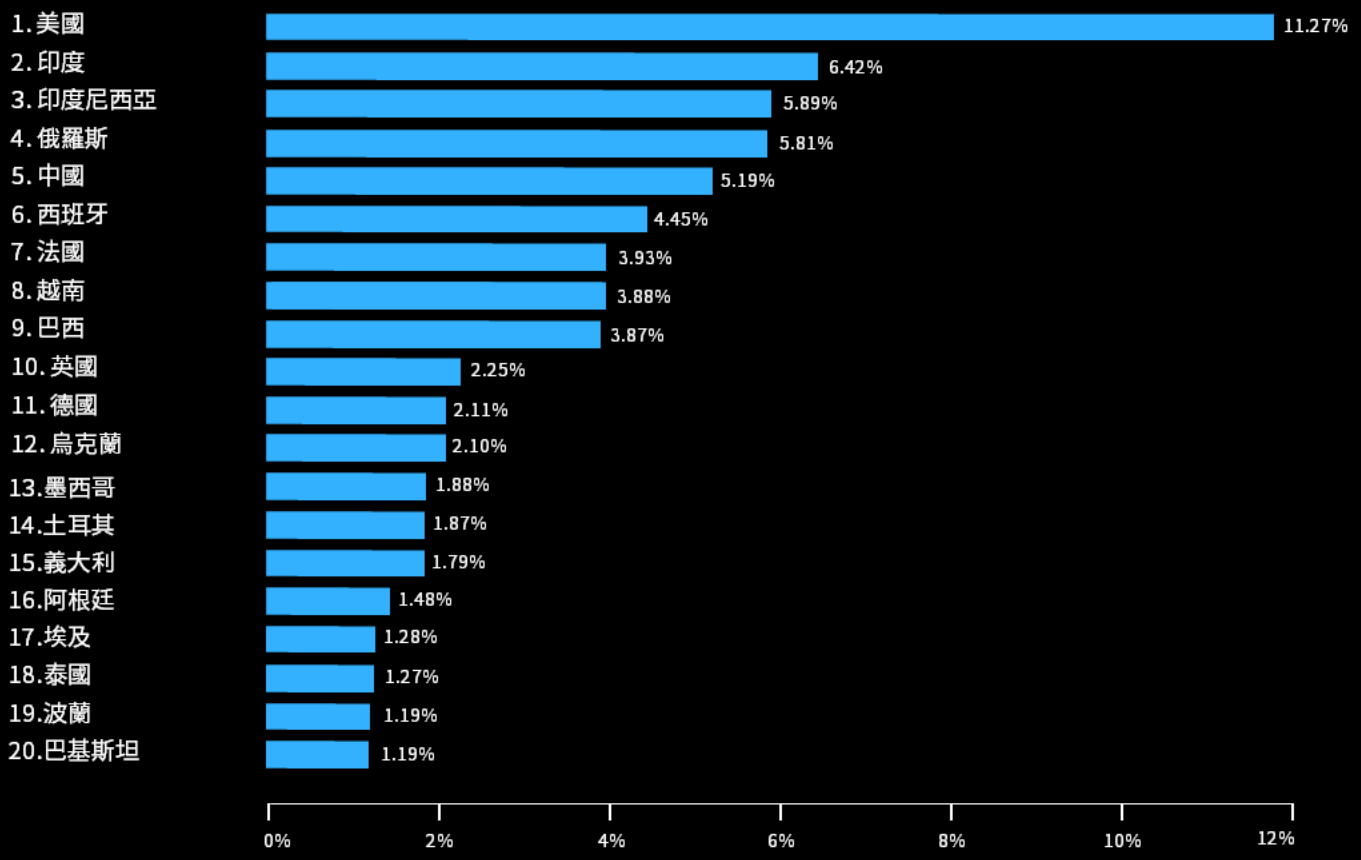
IBM X-Force 透過垃圾郵件殭屍網路的研究，深入瞭解了各種地理位置特定的資料點，這些資料點與垃圾郵件殭屍網路的命令和控制 (C2) 基礎架構密切關聯。我們探尋的其中一個參數就是托管殭屍網路 C2 的地理位置。2019 年，我們發現 C2 主要托管在北美和西歐國家，占 2019 年監測到的所有 C2 實例的一半以上。剩餘的 C2 托管分散在幾個較大的區域。

在許多情況下，垃圾郵件殭屍網路 C2 基礎架構都托管在受影響的伺服器上，並且北美和歐洲伺服器的使用都符合一個共識，即這些國家或地區通常擁有更一致的伺服器正常運作時間。此外，網路犯罪分子更願意攻擊本地資源，當這些伺服器中的流量與目標地理位置的裝置和網路互動時，不太可能釋放危險訊號。

圖 9：

垃圾郵件殭屍網路受害者最多的 20 個國家或地區

2019 年按全球垃圾郵件殭屍網路客戶（受害者）份額排名前 20 位的國家或地區。（來源：IBM X-Force）



按地理區域劃分的垃圾郵件受害者

2019 年垃圾郵件殭屍網路受害者遍佈世界各地，其中美國的受害者人數最多，緊隨其後的是印度、印度尼西亞、俄羅斯和中國。攻擊目標的分佈情況與垃圾郵件製作者的動機一致，即透過大量垃圾郵件活動來吸引儘可能多的收件人。人口較多的國家或地區，垃圾郵件氾濫的程度自然也會更高。

封鎖的惡意網域名稱凸顯了匿名化服務的普遍性

要增加網路的安全性，使其遠離線上威脅，一種常見的做法是防止使用者和資產與潛在或未知的惡意網域名稱進行通訊。為了最大程度降低風險，大多數組織都將可疑的 IP 位址列入黑名單。基於這一想法，開發出在全球範圍內免費提供的網域名稱伺服器 (DNS) 服務 Quad9[3]，它平均每天可阻止 1000 萬個對惡意站點的 DNS 請求。

根據與 IBM Security 威脅情報相關的 Quad9 資料抽樣，垃圾郵件中發現的 URL 占了可疑 DNS 請求的大部分，2019 年占所有請求的 69%。儘管與 2018 年 77% 的比例相比略有下降，但垃圾郵件 URL 仍是最重要的惡意網域名稱類別。之所以有 8% 的下降，可能要歸因於匿名化服務類別，它占到了 DNS 請求的 24%。

垃圾電子郵件仍是最奏效的方式之一，它憑藉龐大的垃圾郵件殭屍網路（如 Necurs 殭屍網路），能夠接觸到最大數量的受害者，每天可傳播數百萬封垃圾電子郵件。惡意網域名稱通常會散佈惡意軟體以分發勒索軟體、憑證竊取指令碼或指向進一步騙局的連結，並且會喬裝成合法品牌或冒充人們知道的品牌來欺騙終端使用者。

垃圾電子郵件中的惡意 URL 連結也是大多數受經濟利益驅動的攻擊者首選的方法，他們可以輕鬆設好騙局，或者選擇地理特定的目標，即便騙局被揭穿，也不會大規模曝光。

圖 10 中的圖表顯示了 2019 年 IBM Security 記錄的惡意網域名稱類型的分佈情況。

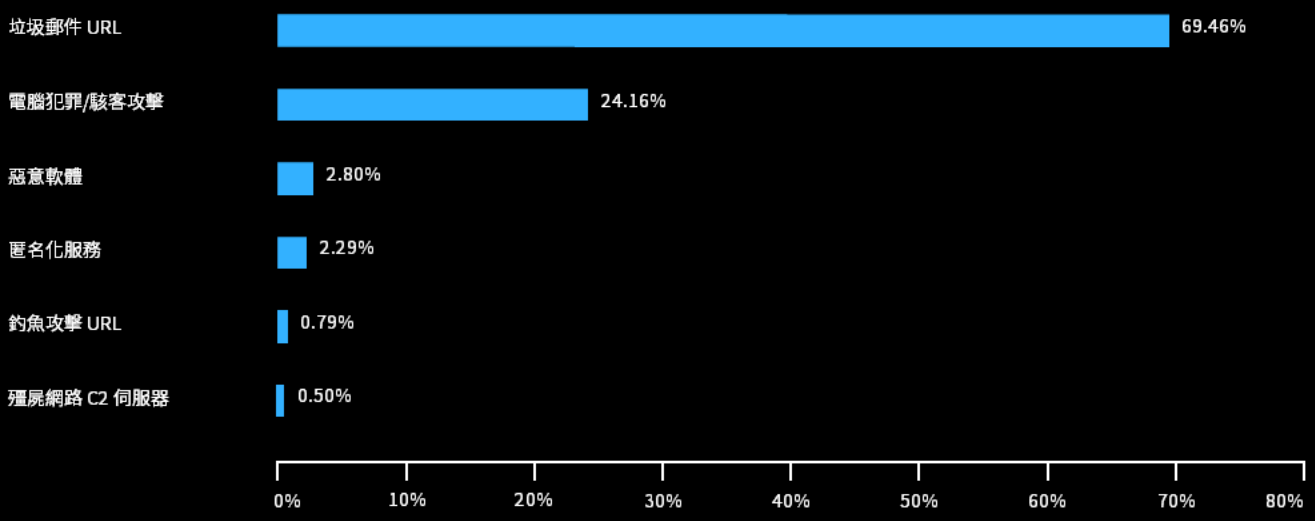
垃圾電子郵件仍是可以接觸到最多潛在受害者的最有效的方式之一。

3 IBM、Packet Clearing House (PCH) 和 Global Cyber Alliance (GCA) 緊密協作，共同創立了 Quad9 並對此提供贊助。

圖 10：

主要的惡意網域名稱威脅類型

2019 年主要惡意網域名稱威脅類型細分，以百分比顯示的 6 種類型（來源：IBM X-Force 和 Quad9）



垃圾郵件 URL：

連結至與垃圾郵件活動相關的站點的網域名稱，它通常是一種屏障，但與進一步的犯罪活動無關

匿名化服務：

連結至匿名化供應商的網域名稱，它會隱藏流量，無法查看

電腦犯罪/駭客攻擊：

明確標識為從事犯罪活動的網域名稱，例如托管網路瀏覽器利用指令碼的網站

釣魚攻擊 URL：

偽裝成其他合法網域名稱，通常是試圖從使用者那裡獲取憑證資料或其他敏感資訊

殭屍網路命令和控制：

連結至殭屍網路活動的網域名稱，可能會感染訪問者

惡意軟體：

托管已知惡意軟體的網域名稱

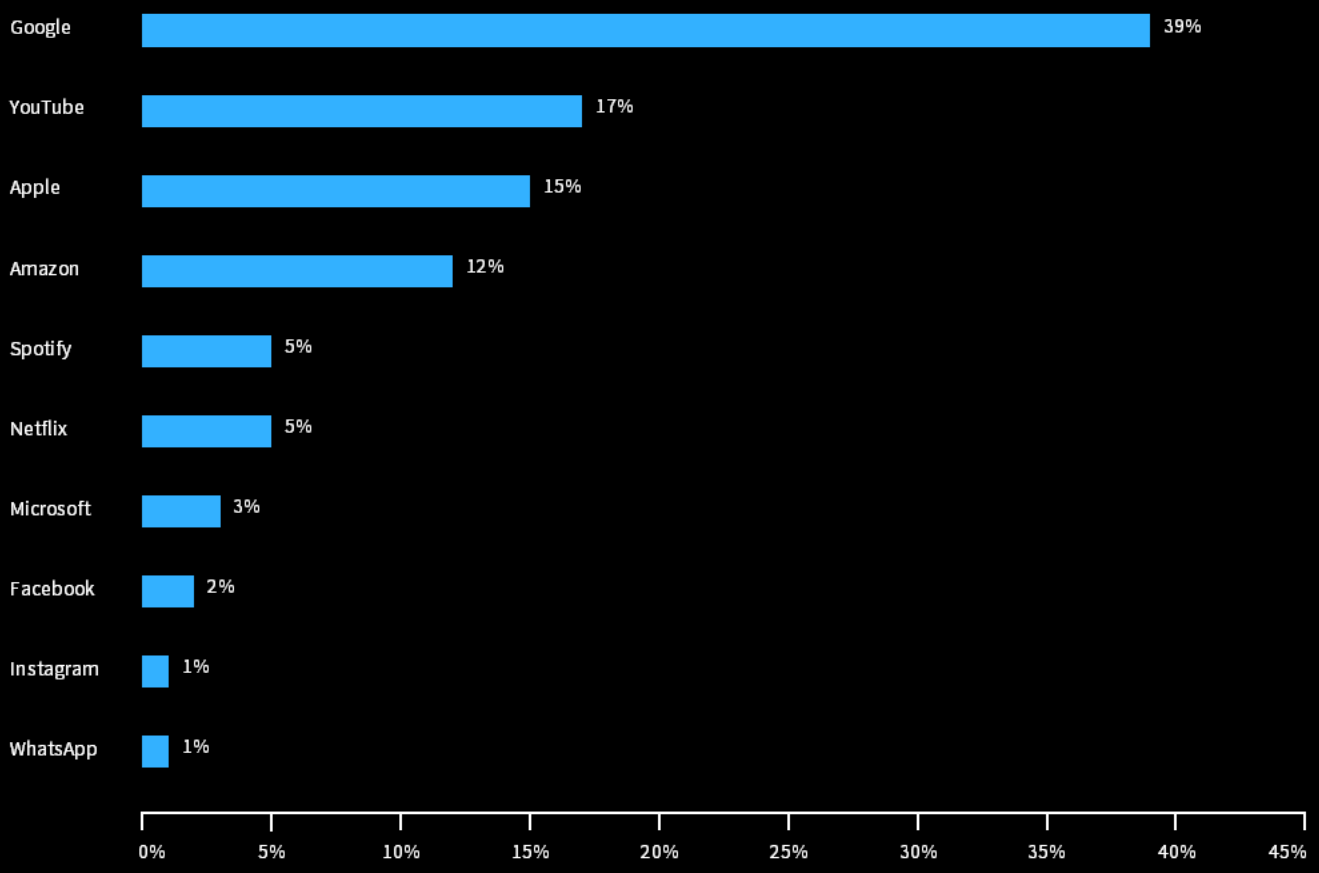
Tor 之類的匿名化服務供應商，允許使用者透過其他威脅實施者營運的節點來匿名處理他們的網路流量來源。儘管匿名化服務可以且經常有合法的目的，例如為使用者的網路瀏覽活動提供更強的隱私保護，這種活動讓使用者更難或根本不可能追蹤並封鎖惡意活動。

匿名化是網路犯罪分子為了掩蓋其行蹤而經常使用的一種伎倆，因為它可以混淆惡意連結，在不觸發資料丟失保護 (DLP) 規則的情況下洩露資料，或者在鎖定遠端伺服器 IP 之前植入更多惡意未經授權使用認證。

4% 的惡意 DNS 請求都來自電腦犯罪或黑帽駭客網頁，其中一些犯罪分子會試圖使用網路瀏覽器散佈關於詐欺的資訊，或從事其他類型的線上犯罪活動。這一比例相對較低，可能是因為這些連結要麼透過匿名化節點進行路由，要麼被公司代理、防火牆偵測並阻止，最後被關閉。

圖 11：
十大被仿冒品牌

2019 年垃圾郵件中被仿冒的 10 大品牌細分，以百分比顯示 10 大品牌（來源：IBM X-Force）



釣魚攻擊者仿冒技術公司、社群媒體

2019 年，釣魚攻擊仍是一個主要的威脅媒介，X-Force 資料顯示，釣魚攻擊活動中最常見的偽冒品牌是科技和社群媒體平台。使用者很難用肉眼分辨出偽冒網域名稱，並且這些網域名稱通常會模仿被仿冒公司使用的合法網域名稱。一個真假難辨的網站如果與「真身」足夠相似，就很容易讓使用者放鬆警惕，在惡意網站上洩露個人資料。

這一資料是透過分析 2019 年由 Quad9 攔截的所有惡意網域名稱，並在 IBM X-Force 網域名稱搶注偵測的基礎上獲得的。

將社群媒體或內容串流網站（例如 Instagram 和 Spotify）作為目標，可能無法向威脅實施者提供易於獲利的資料，例如竊取 Google 或 Amazon 帳戶。但是威脅實施者可以寄希望於個人使用者，希望他們在帳戶與服務之間重複使用密碼，並嘗試使用收集的憑證存取同一使用者持有的更有價值的帳戶。

最常受到攻擊的產業

在當今的威脅情勢下，某些類型的攻擊會因為威脅實施者的動機而具有特殊性，這意味著網路安全風險管理在不同產業間可能會有天壤之別。

為了全面瞭解每年最容易成為攻擊目標的產業，X-Force 研究人員對我們監測到的各產業的攻擊數量進行了排名。根據 X-Force 管理網路提供的攻擊和安全事件資料，從事件回應服務中獲得的資料和洞察以及公開揭露的事件，確定了最常受到攻擊的產業。

圖 12：
十大目標產業

2019 年與 2018 年 10 大最常受到攻擊的產業對比，按攻擊數量計算（來源：IBM X-Force）

產業	2019 年排名	2018 年排名	變化情況
服務	1	1	–
零售	2	4	2
運輸	3	2	-1
媒體	4	6	2
專業服務	5	3	-2
政府	6	7	1
教育	7	9	2
製造	8	5	-3
能源	9	10	1
保健	10	8	-2

圖 12 所示為 2019 年最常受到攻擊產業及其相比 2018 年變化情況的對比圖。

不難看出，金融服務業排名靠前，零售業也愈發受到攻擊者的「青睞」。媒體和娛樂公司、教育以及政府機構同樣也是如此。

下面的章節將根據各種資料來源深入分析目標攻擊的相對頻率，以及我們在 2019 年針對每個產業的調查結果。有些產業的描述凸顯了近年來格外活躍地攻擊某一產業的威脅實施者，但此清單並不詳盡，只包括 2019 年之前的資料。X-Force IRIS 追蹤並概述了數十個民族國家贊助的網路犯罪組織。未分類的活動和自然狀態下發現的活動都在活動「HIVE」中進行追蹤。活動達到了嚴格的分析閾值之後，就會過渡到 IBM Threat Group (ITG)，其依據是一系列 TTP、基礎架構、目標以及間諜情報技術。

金融與保險

2019 年，金融保險業連續第四年在最容易受到攻擊的產業排行中榜上有名。在前 10 大目標產業中，對這一產業發起的攻擊占到了所有攻擊的 17%。

在經常針對金融實體發起攻擊活動的網路威脅實施者中，利慾熏心的網路犯罪分子占有最大的比重，金融公司對網路犯罪分子的吸引力顯而易見：可能迅速獲得高額回報，一旦得手就能將數百萬美元收入囊中。

X-Force 事件回應活動的資料顯示，儘管公開揭露的資料洩露較少，金融保險仍是最容易受到攻擊的產業。

這表明，相對於其他產業而言，金融保險公司會遭遇更多攻擊，但他們也會採取更有效的工具和流程，在攻擊活動釀成重大事件之前發現並遏制威脅。金融公司也更願意測試他們的回應計畫，並且在使用 IBM Security Command Centers 來準備應對網路攻擊的組織中，大部分都是金融公司。由 Ponemon Institute 執行並由 IBM Security 贊助的 2019 年資料洩露成本報告[4] 稱，針對相關場景廣泛測試事件回應計畫和團隊，可有效規避因為資料洩露造成的經濟損失。舉例來說，在網路範圍內對其事件回應計畫進行了廣泛測試的組織遭到破壞，其平均損失要比 392 萬美元的資料洩露總體平均成本少 32 萬美元。

2019 年針對金融業組織的主要威脅團體是 ITG03(Lazarus)、ITG14 (FIN7) 和不同的 Magecart 派系。TrickBot、Ursnif 和 URLZone 等銀行木馬是 2019 年令銀行深受困擾的頭號威脅，這些木馬會接管並詐欺客戶帳戶。

4 由 Ponemon Institute 執行並由 IBM 贊助的年度資料洩露成本報告。

零售

2019 X-Force 資料顯示，零售業遭受的攻擊在所有產業中排名第二。在前 10 大產業中，零售業所遭受的攻擊占 16%，與 2018 年排名第四的 11% 相比有所上升。2019 年，零售業遭遇的網路攻擊數量排名第二。

根據 X-Force IRIS 提供的資料和公開揭露的資料洩露資訊，零售業在 2019 年排名第二。最常見的以零售業作為攻擊目標的威脅實施者是受經濟利益驅動的網路犯罪分子，他們瞄準零售業，是為了竊取消費者的個人識別資訊 (PII)、支付卡資料、金融資料、購物歷史記錄以及忠誠計畫資訊。犯罪分子經常利用這些資料接管客戶帳戶，欺騙客戶並在各種身分竊取場景中重新利用該資料。

網路犯罪分子在 2019 年針對零售商的一種常用攻擊伎倆是銷售點 (POS) 惡意軟體和電子商貿支付卡竊聽，每種攻擊都在透過物理支付終端或線上交易時竊取支付卡資訊。

尤為值得一提的是，一組歸屬於 Magecart 的網路犯罪派系一直將第三方支付平台和知名的線上零售商作為攻擊目標，直接將惡意 JavaScript 程式碼注入其網站的卡支付頁面。該程式碼在結帳過程中執行，會將受害者的支付卡資訊傳輸給網路犯罪分子，此外，還可以獲取目標供應商的資訊。

X-Force IRIS 事件回應人員在 2019 年的多次洩露中監測到了此類攻擊，同時表示，儘管惡意程式碼片段可能微不足道，但針對基礎平台的後端破壞可能會牽一髮而動全身，使得犯罪分子能夠使用相同的技術攻擊數千家商店。

攻擊零售業的主要威脅團夥包括：

ITG14 (FIN7)HIVE0065 (TA505)ITG08 (FIN6)Hive0038 (FIN6)	Hive0061 (Magecart 10)
Hive0040 (Cobalt Gang)Hive0053 (Magecart 2)	Hive0062 (Magecart 11)
Hive0054 (Magecart 3)	Hive0066 (Magecart 12)
Hive0055 (Magecart 4)	Hive0067 (FakeCDN)
Hive0056 (Magecart 5)	Hive0068 (GetBilling)
Hive0057 (Magecart 6)	Hive0069 (Illum Group)
Hive0058 (Magecart 7)	Hive0070 (PostEval)
Hive0059 (Magecart 8)	Hive0071 (PreMage)
Hive0060 (Magecart 9)	Hive0072 (Qoogle)
	Hive0073 (ReactGet)
	Hive0083 (Inter Skimmer)
	Hive0084 (MirrorThief)
	Hive0085 (TA561)

除了線上電子商貿 Skimmer 惡意程式外，銷售點惡意軟體仍是網路犯罪分子在零售商實體店的慣用手段，伺機在交易過程中或在將資料寫入記憶體時竊取銷售點機器和後端伺服器中的支付卡資料。

運輸

運輸業是任何國家或地區的重要基礎設施中必不可少的一部分。從事該產業的公司透過三種主要運輸方式（包括陸運，海運和空運）提供工業和消費者服務，從而推動經濟發展。運輸業是 2019 年第三大目標產業，攻擊頻率從 2018 年的 13% 下降至 2019 年的 10%。

運輸業緊隨金融和零售業之後排名第三，可以看出運輸公司營運的資料和基礎設施愈來愈有吸引力。無論是網路犯罪分子還是民族國家威脅實施者，都對這些資產虎視眈眈。運輸公司擁有的資訊成為了網路犯罪分子眼中誘人的「蛋糕」，這些資訊包括個人識別資訊、履歷資訊、護照號碼、忠誠計畫資訊、支付卡資料和旅行路線等。

在運輸業，尤其是航空公司和機場，更是網路犯罪分子和民族國家對手日益青睞的目標，他們希望追蹤感興趣的旅行者，或者在暗網上出售旅行者的個人資料，以此方式坐收漁利。

與其他產業相比，運輸業的網路威脅往往伴隨著更高的風險，因為攻擊可能會產生潛在的蝴蝶效應，讓人們面臨生命危險，並且有可能對依賴運輸服務來開展營運的其他產業產生連鎖影響。

2019 年對運輸業發起攻擊的威脅實施者團夥有所不同，網路犯罪團體和民族國家對手都對全球的運輸組織發起了攻擊。

攻擊運輸業的主要威脅團夥包括：

ITG07 (Chafer)	ITG17 (Muddywater)
ITG09 (APT40)	Hive0016 (APT33)
ITG11 (APT29)	Hive0044 (APT15)
ITG15 (Energetic Bear)	Hive0047 (Patchwork)

媒體與娛樂

根據 X-Force 的攻擊目標排名，排名第四的是媒體業，該產業受到的攻擊在前十大產業的所有攻擊中占 10%。媒體業的占比與 2018 的 8% 相比有所上升，排名從第六位升至第四位。

媒體業包括許多知名的子產業，例如電信公司，以及生產、處理和分發新聞媒體和娛樂的公司。對於試圖影響公眾輿論、控制資訊流或保護其組織或國家聲譽的網路攻擊者來說，媒體和娛樂產業是一個高價值目標。具體來說，民族國家團隊可以將負面的媒體內容視為對其國家安全的重大威脅，而網路罪犯則發現，對媒體和娛樂產業的攻擊可以獲取豐厚的回報，因為他們可以憑藉竊取未播出的媒體內容勒索贖金。

2019年，機會主義網路犯罪分子和民族國家對手通常會將目標鎖定在這一產業。

攻擊媒體與媒體業的主要威脅團夥包括：

ITG03 (Lazarus)
Hive0003 (Newscaster)
Hive0047 (Patchwork)

專業服務

專業服務業是指專門為其他產業提供專業諮詢服務的公司，比如一些提供法律服務、諮詢、HR 和專業客戶支持的公司，都屬於這一產業。X-Force 資料顯示，專業服務業遭受的攻擊數量在 10 個產業所有攻擊中的占比為 10%，與 2018 年的 12% 相比略有下降。

公開揭露的資料洩露資訊表明，在排名的所有產業中，專業服務洩露的記錄數量最多。這些公司當中有很多都會從客戶那裡獲取高度敏感的資料，例如法律訴訟資料、用於會計和稅務的資料，對於那些一心想要謀取錢財或內部資訊的攻擊者而言，這些都是充滿誘惑力的目標。

此外，該產業還包括一些技術公司，他們因為擁有第三方存取權限而受到愈來愈多的關注，攻擊者可以利用他們去破壞這些公司所服務的更大、更安全的組織。

此外，專業服務公司的日常工作流也便於犯罪分子透過釣魚攻擊電子郵件和惡意巨集來建立攻擊媒介。許多專業服務公司高度依賴生產力檔案（例如 Word 和 Excel 文件附件）來簽訂合約、與客戶溝通以及完成日常工作任務。巨集的使用是網路犯罪分子利用的最臭名昭著的攻擊媒介之一，他們將惡意指令碼植入此類檔案中，任何組織都無法徹底攔截此類指令碼。

2019 年對專業服務發動攻擊的知名威脅實施者團夥：ITG01 (APT10, Stone Panda)，一個可能起源於中國的民族國家贊助團體。

政府

在我們的排名中，政府產業是第六大最常受到攻擊的產業，其攻擊數量在前 10 大產業中占 8%，這一比例與去年持平，但排名比 2018 年（第七名）略有上升。

政府部門是一個充滿誘惑力的高價值目標，民族國家網路威脅實施者希望從中獲得領先於對手的優勢，駭客活動分子希望從中獲得機密資訊或者證明自己的技術實力，網路犯罪分子希望透過勒索或竊取資料謀取錢財。

近年來，市政府受到的攻擊尤為猛烈，因為他們的安全性低於私有企業，網路犯罪分子看準了這一軟肋，希望從中勒索錢財。在威脅實施者眼中，政府實體擁有大量寶貴資產，其中主要是機密資訊和可能的國家機密，包括政府雇員和代理人的個人識別資料、財務資訊、內部通訊以及關鍵網路的功能。

民族國家威脅實施者向來對政府部門實體虎視眈眈，X-Force IRIS 評估稱，他們最有能力發起攻擊。但在 2019 年，網路犯罪組織也愈來愈多地將目標對準政府實體，試圖加密和把持政府正常運作所需資料以期勒索贖金，在省市一級更是如此。

2019 年，僅在 1 月到 7 月之間，就有 70 多個政府實體受到勒索軟體的攻擊。網路犯罪分子還竊取了資料（包括來自國防網站的資料），然後將資料洩露到暗網上。臭名昭著的駭客分子發現政府是一個有吸引力的目標，尤其是當他們希望就有爭議的問題發表聲明時更是如此。與私營企業相比，政府組織的網路安全資金水準往往略遜一籌，但他們仍需要為選民提供一致的服務，這便進一步加劇了威脅實施者對這些組織的挑戰。

2019 年，針對政府機構發起攻擊的知名威脅實施者團夥：各種網路犯罪參與者和民族國家贊助的團體。

教育

教育業受到的攻擊數量在前 10 大產業中占 8%，與 2018 年的 6% 相比略有上升，成為排名第七的最常受到攻擊的產業。

教育業擁有大量寶貴資產，受經濟利益驅動的威脅實施者和民族國家威脅實施者對這些資產覬覦已久。從智慧財產權 (IP) 到 PII，教育組織永遠是各類威脅實施者眼中的一塊肥肉。

敵對實施者各懷鬼胎，使用不同的初始感染媒介破壞學術機構網路，但我們的監測結果顯示，最常見的方法仍是釣魚攻擊電子郵件，且通常會是針對特定的學術機構或研究領域量身定制的釣魚攻擊電子郵件。

教育業組織通常有著龐大而多樣化的 IT 基礎架構和數位足跡。他們掌控著不同的資產，為數量不斷攀升的使用者提供服務，其中有職員、學生，也有承包商。攻擊面如此廣泛，要保障其安全更是難上加難，威脅實施者便趁機開展各種惡意活動。2019 年 10 月份發佈的報告顯示，單單在美國，2019 年就至少有 500 所學校遭受了網路攻擊，其中大多數都是勒索軟體發起的攻擊。

教育業一些值得關注的更複雜的攻擊包括：民族國家威脅實施者入侵大學網路，然後將它們作為集結地，大肆感染媒體組織和軍事承包商。同樣，以美國資助的研究作為攻擊目標的攻擊者，也會絞盡腦汁入侵大學網路，伺機竊取一些價值連城的智慧財產權。

攻擊教育業的主要威脅團夥包括：

ITG05 (APT28)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive0075 (DarkHydrus)

IBM X-Force IRIS 公佈了一項有高度把握的評估結果，宣稱受經濟利益驅動的威脅實施者和隸屬於政府部門的威脅實施者為了獲取重要資訊，會繼續將此產業作為攻擊目標。

2019 年此產業的知名威脅實施者團夥包括：投機取巧的網路犯罪勢力和來自中國、俄羅斯和伊朗的民族國家對手。

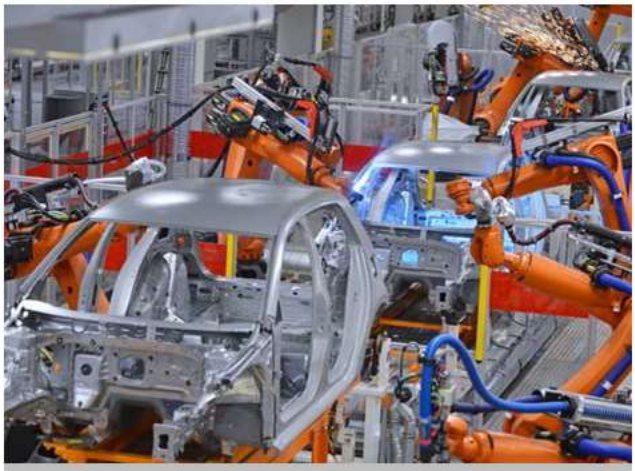
製造

製造商透過金屬、化工、生產資料和電子產品推動經濟發展，但也不能免於各種 IT/OT 威脅。在前 10 大最常受到攻擊的產業中，製造業所遭受的攻擊數量占 8%，排名第八，與 2018 年的 10% 相比有所下降。

製造業所遭受的攻擊數量比上一年要少，數字的下降反映出一個事實，即：在很多情況下，製造業的資料洩露都未涉及到必須合法揭露且受到法規監管的資訊。因此，有些攻擊並未公開揭露，這樣一來，儘管製造商受到了攻擊，但揭露的數量卻少於實際數量。

製造商也會營運 IT 和 OT 環境，因此也同樣面臨著影響 ICS 和 SCADA 系統的威脅。不過，儘管該產業的資訊安全在過去一直落後，但挪威製造商對 2019 年一次成功的重大勒索軟體攻擊的公開回應，卻可能表明該產業正在改變其網路安全方法。

尋求經濟利益和智慧財產權的網路犯罪分子或民族國家威脅實施者可能對製造業的公司構成最大的網路威脅。2019 年針對製造商的最常見攻擊手段之一是商務電子郵件入侵 (BEC) 欺詐，如果他們經常與外國供應商開展業務，則更是雪上加霜。在這種情況下，攻擊者會破壞公司的電子郵件伺服器，甚至是電子郵件帳戶，攻擊者會將自己插入現有的通訊執行緒中，最終將數百萬美元轉移到他們控制的帳戶中。



針對製造業發起攻擊的知名威脅團夥包括：

ITG01 (APT10)
ITG09 (APT40)
HIVE0006 (APT27)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0076 (Tick)

此外，製造商還容易受到供應鏈攻擊，民族國家對手可能會利用供應鏈在他們製造的產品中植入後門或惡意軟體，然後再將其運送到其他國家或地區。

在財務動機方面，攻擊者可能將製造商作為獲取商業秘密和智慧財產權的目標。組織花費數年時間開發的研究可以迅速為暗網中的網路罪犯帶來利潤，或者提升一個國家的經濟或國防優勢 - 對國防和軍事裝置製造商而言更是如此。

X-Force 資料顯示，勒索軟體、釣魚攻擊和 SQLi 注入攻擊也會經常攻擊製造業。

能源

2019 年，能源行業是第九大最常受到攻擊的產業，它所遭受的攻擊數量在 10 大產業的總攻擊和事件數量中占 6%。這一產業排名與 2018 年持平，2018 年遭受的攻擊數量也占總數量的 6%。

能源行業的公司備受網路攻擊的青睞，部分原因在於，這些公司重要性高，堪稱各國重要基礎設施的支柱。各種形式的能源對經濟、國家安全以及城市和產業的日常運轉有著舉足輕重的作用。

對能源行業發動攻擊的目標可能各不相同。能源公司一些利潤豐厚的資產，例如客戶資料、財務資料、商業機密和專利技術資訊等，其價值與其他產業公司的資產不相上下。

真正讓能源行業與眾不同的是，ICS 系統和管理它們的 SCADA 系統可能受到物理破壞。對於希望監視或控制目標設施操作的對手而言，這些系統是非常有價值的目標；舉例來說，當涉及到網路戰，而且關係到競爭對手國家的核設施時，尤其如此。該產業還會受到破壞性惡意軟體（例如 ZeroCleare）的攻擊。

以中斷 ICS 系統運作為目的而發起的攻擊一旦成功，就可能對依賴能源行業提供的電力、天然氣、石油或其他資源的客戶造成毀滅性影響。在曾經針對烏克蘭發電廠發起的一系列事件中，都可以看到此類攻擊以及由此產生的嚴重後果，據稱這些攻擊是由俄羅斯發起，目的是要進行物理破壞。

攻擊能源行業的主要威脅團夥包括：

ITG01 (APT10)	HIVE0006 (APT27)
ITG09 (APT40)	Hive0016 (APT33)
ITG07 (Chafer)	Hive0044 (APT15)
ITG11 (APT29)	Hive0045 (Goblin Panda)
ITG12 (Turla Group)	Hive0047 (Patchwork)
ITG13 (APT34)	Hive0076 (Tick)
ITG15 (Energetic Bear)	Hive0078 (Sea Turtle)
ITG17 (Muddywater)	Hive0081 (APT34)
Hive003 (APT35)	

醫療保健

醫療保健業是第十大目標產業，所遭受的攻擊占 10 大產業所有攻擊數量的 3%，與 2018 年的排名第八和 6% 的攻擊相比略有下滑。

大量證據表明，利慾熏心的網路犯罪分子是醫療保健業網路和醫療設備的主要攻擊者，他們的目的是竊取病歷，然後在暗網上出售，或者是加密網路連接的裝置，以干擾活動並挾持公司以勒索資金 。

醫院和療養院網路中斷會迫使醫療機構支付勒索軟體攻擊費用，以儘快恢復網路營運並保障患者生命安全。有時候贖金會高到離譜，例如 2019 年攻擊者發起 Ryuk 攻擊之後索要了 1400 萬美元的高額贖金。

2020 年，醫療保健業會繼續改進其安全措施以增強資料保護。鑒於勒索軟體攻擊頻繁發生，醫院必須增強事件回應能力，並防範針對一些不安全的醫療設備發起的新攻擊，這些攻擊很容易讓醫院束手就擒並被心懷不軌的攻擊者所左右。

對本產業發起攻擊的知名威脅團夥包括一些受經濟利益驅動的網路犯罪團夥，例如操作 Ryuk 勒索軟體的團夥。儘管勒索軟體攻擊的確凸顯了當醫院受到感染時可能發生的危機，但民族國家威脅實施者對此領域的興趣並不持久。

全球中心洞察

2019 年，威脅實施者的攻擊目標遍佈所有地區，且北美、亞洲和歐洲的活動最為頻繁。

X-Force 研究人員還發現，在 2019 年針對中東和南美的威脅實施者活動中，前者遭受的駭客活動分子和民族國家攻擊更多，而南美則主要受到追逐經濟利益的威脅實施者的攻擊。

在本節中，我們將更深入地研究發生在這些地域的攻擊，以更好地瞭解 X-Force 所監測到的攻擊的特性，側重於各個領域的主要威脅實施者以及 2020 年要留意的重要日期，提防可能會增加的威脅實施者活動。對於一些地區，我們突出顯示了近年來在該地區格外活躍的威脅實施者，但該清單並不詳盡，只列出了 2019 年之前的資料。

本節使用了如上所述的 IBM Threat Group 命名方法，還利用了 IBM 全球事件回應中的資料以及公開揭露的洩露資料。

北美

北美有很多潛在目標，還擁有大量網際網路基礎架構，是令犯罪實施者垂涎的攻擊目標。2019 年，北美洩露的記錄超過 50 億條。

北美在威脅實施者攻擊的所有類別中排名最高，占 2019 年所有事件中的 44%。

2019 年，IBM 對多起北美事件做出了回應，發現這些事件都使用了商品化的惡意軟體 - 可以在地下市場上購買或免費獲得的程式碼。商品惡意軟體可能很難識別，卻能快准狠地達成犯罪目標。

2019 年，向北美發起的民族國家威脅實施者活動保持不變，但未監測到重大事件。近來美中之間的貿易談判可能會增加對在中美兩國開展業務的組織的攻擊，只要談判尚無結果，這些組織就應保持警惕。

即將舉行的具有重大網路安全歷史意義的活動：

7 月 13 日
（美國民主黨全國代表大會）
8 月 24 日
（美國共和黨全國代表大會）
11 月 3 日
（美國總統選舉）

對此地區發起攻擊的威脅實施者團夥包括：

ITG05 (APT28)
ITG08 (FIN6)
ITG11 (APT29)
ITG15 (Energetic Bear)
Hive0082 (Cobalt Dickens)
Hive0042 (Kovter)
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0006 (APT27)
Hive0003 (APT35)
ITG01 (APT10)
ITG03 (Lazarus)
ITG04 (APT19)
ITG09 (APT40)
ITG07 (Chafer)

2019 年 X-Force 事件回應活動中監測到的最突出的攻擊活動：

商務電子郵件入侵、勒索軟體、以金融業為目標的民族國家攻擊活動。

亞洲

X-Force 分析結果顯示，亞洲獲得了第二高的風險評等，在公共洩露事件中排名第二，事件數量占 2019 年總數量的 22%。2019 年，亞洲洩露的記錄超過 20 億條，僅次於北美。

有大量威脅實施者都以亞洲的組織作為攻擊目標，其中以朝鮮半島、日本和中國尤為突出。在亞洲監測到的許多攻擊都採用了民族國家威脅實施者 TTP。ITG10 便是其中之一，可能是對韓國實體發起攻擊的朝鮮威脅實施者。另一個便是 ITG01，可能是針對日本發起攻擊的中國威脅實施者。

近期在亞洲發生的地緣政治事件增加了在該地區民族國家發起活動的可能性。中國香港爆發的民主抗議和隨後的鎮壓讓中國陷入不安之中。朝鮮與其鄰國間劍拔弩張的局面讓這些活動更加猖獗。印度對克什米爾地區的蠶食同樣導致該地區緊張局勢加劇。

進入 2020 年，對這些潛在的不穩定地緣政治風險的監測對於瞭解在該地區營運的組織所面臨的風險至關重要。

即將舉行的具有重大網路安全歷史意義的活動：

7 月 24 日
（2020 年東京奧運會）

10 月 10 日
（中國台灣獨立日）

對此地區發起攻擊的威脅實施者團夥包括：

Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0049 (Samurai Panda)
ITG01 (APT10)
ITG03 (Lazarus)
ITG05 (APT28)
ITG06 (APT30)
ITG09 (APT40)
ITG10 (APT37)
ITG11 (APT29)
ITG16 (Kimsuky)
Hive0016 (APT33)
Hive0040 (Cobalt Gang)
Hive0047 (Patchwork)
Hive0063 (DNSpionage)
Hive0076 (Tick)
Hive0079 (Labryinth Cholima)
Hive0006 (APT27)
Hive0003 (APT35)
ITG15 (Energetic Bear).

2019 年 X-Force 事件回應活動中監測到的最突出的攻擊活動：

PowerShell 攻擊、內部人員威脅、勒索軟體。

歐洲

歐洲淪為與亞洲相似的惡意活動受害者，事件數量占總數量的 21%。

亞洲受到的攻擊大多來自對手國，歐洲則不同，它們受到的攻擊主要來自受經濟利益驅動的威脅實施者。之所以存在這種差異，可能是因為根據貨幣匯率，從歐洲公司竊取資訊的可能性更大。另外，其犯罪動機可能是為了竊取智慧財產權，然後將其出售給競爭對手以獲取鉅額利潤。

進入 2020 年，英國脫離歐盟（脫歐）可能會在駭客活動分子圈內產生連鎖反應，但 2019 年並未監測到攻擊活動。此外，主要歐盟國家（德國、法國）即將到來的大選活動，也可能成為希望利用政治在這些國家興風作浪的民族國家威脅實施者的目標。

即將舉行的具有重大網路安全歷史意義的活動：

1 月 31 日
（英國根據第 50 條規定退出歐盟）
6 月 28 日
（烏克蘭憲法日/NotPetya 紀念日）

對此地區發起攻擊的威脅實施者團夥包括：

ITG05 (APT28)
ITG08 (FIN6)
ITG12 (Turla)
ITG15 (Energetic Bear)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG14 (FIN7)
ITG17 (Muddywater)
Hive0006 (APT27)
Hive0003 (APT35)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0063 (DNSpionage)

2019 年 X-Force 事件回應活動中監測到的最突出的攻擊活動：

RDP 入侵、POS 惡意軟體、內部人員威脅。

中東

2019 年，X-Force IRIS 監測到了大量與民族國家關聯的事件，給中東的許多組織帶來了影響，但 2019 年威脅實施者活動的總體指標仍相對較低，該地區的事件占 7%。

活動減少的原因有很多，例如其他地區可以為網路犯罪活動帶來更高的投資回報等。但是，與其他地區的不同之處在於，與世界其他地區相比，中東的駭客活躍分子和民族國家活動比例較高。

2019 年，駭客分子活動引發了政治動亂，發生了多起涉及伊朗的重大事件。同樣，民族國家活動，例如打著追求伊朗國家利益旗號的 ITG13，透過在該地區發動破壞性攻擊，對從事金融業的組織發起攻擊。

葉門的政治動盪和持續武裝衝突繼續帶來網路威脅活動的風險，衝突各方都在利用網路攻擊來傳播其資訊並創造收入。這些風險很可能會持續到 2020 年，因為各方在這場持續不斷的衝突中仍在不斷地公開威脅對方。

即將舉行的具有重大網路安全歷史意義的活動：

11 月 21 日
（2022 俱樂部世界盃足球賽，卡達）

對此地區發起攻擊的威脅實施者團夥包括：

Hive0044 ITG07
(Chafer) ITG13
Hive0081 (APT34
Hive0078 (Sea Turtle)
Hive0075
(DarkHydrus)
Hive0063 (DNSpionage)
Hive0047 (Patchwork)
Hive0022
(Gaza Cybergang)
Hive0016 (APT33)
Hive0006 (APT27)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG10 (APT37)
ITG09 (APT40)
ITG05 (APT28)
ITG01 (APT10)

2019 年 X-Force 事件回應活動中監測到的最突出的攻擊活動：

破壞性惡意軟體、DDOS 攻擊、Web 指令碼攻擊。

南美

2019 年，南美洲也與嚴重的網路犯罪活動展開了殊死較量，但它並未獲得與另外三個重點地區相同的關注度，事件數量僅占總數量的 5%。然而，該地區的活動仍在逐年增加，X-Force 監測到重大事件回應活動有所增加，在零售和金融服務業尤為突出。

此地區監測到的事件中有勒索軟體活動，該活動在 2019 年一直處於增長狀態。

即將舉行的具有重大網路安全歷史意義的活動：

6 月 12 日
（2020 年美洲盃足球賽，哥倫比亞和阿根廷）

對此地區發起攻擊的威脅實施者團夥包括：

Hive0081 (APT34)
Hive0044 (APT15
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29) ITG05 (APT28)
ITG03 (Lazarus) ITG01 (APT10)

2019 年 X-Force 事件回應活動中監測到的最突出的攻擊活動：

商務電子郵件入侵、勒索軟體、以金融業為目標的民族國家攻擊活動。

為 2020 年的彈性應對做好準備

根據 IBM X-Force 在此報告中揭示的重要發現，無論從事哪種產業，也無論在哪個國家或地區經營業務，只有充分瞭解最新威脅情報並培養強大的回應能力，才能在不斷變化的威脅格局中規避威脅。

我們的團隊為每個組織推薦了一系列舉措，使其能夠在 2020 年更好地應對網路威脅：

－利用威脅情報，以更好地瞭解威脅實施者的動機和策略，進而對安全資源進行優先級排序。

－在您的組織內組建事件回應團隊並開展培訓活動。如果不能組建團隊，就掌握一種有效的事件回應能力，以確保及時回應有重大影響的事件。2019 年，IBM Security 監測到，及時遏制影響可顯著削減相關成本，因為我們的團隊及時干預 MegaCortex 感染活動，中途阻斷了勒索軟體攻擊，進而避免了數千美元的損失。

－對您組織的事件回應計畫開展壓力測試，以形成肌肉記憶。桌面演習或網路突擊體驗可以為您的團隊提供重要的經驗，進而有助於縮短回應時間，減少停機時間，最後做到即便發生洩露也能降低損失。

- 實施多重要素身分驗證 (MFA) 仍然是組織最有效的安全優先事項之一。2019 年，憑證盜竊或重複使用是威脅實施者最常用的攻擊手段之一，MFA 可以有效地防患於未然，掐斷攻擊的苗頭。

- 因為普遍利用釣魚作為攻擊媒介，請確保組織制定適當的解決方案（例如 Quad9）來偵測和攔截欺騙性網域名稱。

- 及時備份，測試並離線儲存備份。不僅要將備份落到實處，還要透過真實的測試來驗證備份的有效性，這對確保組織的安全性至關重要。

未來展望及關鍵要點

2020 年，組織需要密切關注新威脅，同時也要警惕一些舊威脅。

- 2020 年，風險面會繼續增長，目前已有超過 15 萬個漏洞，還會有新漏洞被不斷發現。
- 2019 年洩露的記錄數量是 2018 年的四倍，2020 年仍會有大量記錄因為洩露和攻擊而丟失。
- 隨著物聯網裝置，營運技術 (OT) 以及互聯的工業和醫療系統愈來愈多，威脅實施者會繼續物色不同的攻擊媒介。
- 威脅實施者對惡意軟體的使用會繼續波動，2019 年，勒索軟體、加密貨幣挖礦軟體以及殭屍網路都曾「風光無限」。我們預計 2020 年會繼續保持這種趨勢，這就意味著，組織需要讓自己遠離各種隨著時間不斷變化的威脅。
- 勒索軟體和加密貨幣挖礦軟體的高等級程式碼創新，意味著這些威脅在 2020 年會不斷演變，組織需要具備更好的偵測和遏制能力。
- 垃圾郵件活動會繼續肆虐，需要組織更加勤奮地制定黑名單，修補漏洞並監控威脅。
- 產業特定目標的逐年變化凸顯了所有產業的風險，也更需要更先進、更成熟的網路安全計畫。
- 組織可以利用其地理位置來確定最有可能的攻擊者和攻擊動機，以預估並減輕他們可能面臨的一些相關風險。

關於 X-Force

IBM X-Force 致力於研究和監測最新的威脅趨勢，向客戶和公眾普及新興威脅及關鍵威脅方面的知識，同時交付安全內容，幫助 IBM 客戶實現安全防護。

從基礎架構、資料和應用保護到雲端及托管安全服務，IBM Seurity Services 擁有豐富的專業知識，可幫助您保護關鍵資產。

IBM Security 目前正在為一些全球最先進的網路保駕護航，並延請了大量的優秀人才為其服務。

致謝

Michelle Alvarez
Dave Bales
Joshua Chung
Scott Craig
Kristin Dahl
Charles DeBeck
Ari Eitan (Intezer)
Brady Faby (Intezer)
Rob Gates
Dirk Harz
Limor Kessem
Chenta Lee
Dave McMillen
Scott Moore
Georgia Prassinos
Camille Singleton
Mark Usher
Ashkan Vila
Hussain Virani
Claire Zaboeva
John Zorabedian

瞭解有關 IBM Security 的更多資訊

免費咨詢熱線：0800-016-888 按 1

服務時間：9:00-17:00

IBM Security
New Orchard Rd
Armonk, NY 10504
美國印刷
2020 年 2 月

美國印刷
2020 年 2 月

IBM **Securit**