

2020 年 ICS 端點威脅報告

Matsukawa Bakuei、Ryan Flores、Lord Remorin 與 Fyodor Yarochkin



TREND
MICRO™



research

趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

出版者：

Trend Micro Research

作者：

Matsukawa Bakuei、Ryan Flores、
Lord Remorin 與 Fyodor Yarochkin

圖片授權：Shutterstock.com

獻給 Raimund Genes (1963-2017 年)

內容

4

高階主管摘要：研究發現

5

定義與資訊揭露

8

執行 ICS 軟體的端點所面臨的惡意程式威脅

17

結論


18

建議

20

入侵指標資料





近幾年來，隨著 IT 面的業務流程與 OT 面的實體流程越來越緊密連結，工業控制系統 (ICS) 的資安也開始成為大家的目光焦點。雖然這樣密切連結提升了可視性、效率及速度，但也意外地讓 ICS 暴露在 IT 網路數十年來所面對的資安威脅中。

為了驗證 ICS 的資安情勢並且為全球建立一套基準來檢視這些系統所面臨的威脅，本文分析並列舉了一些專門攻擊 ICS 端點的惡意程式家族。

根據網路犯罪集團在攻擊事件中所運用的惡意程式類型，我們就能看出這類網路攻擊的範圍和嚴重性，進而提供有關駭客與受害網路的重要線索。

從駭客所選擇的惡意程式，就能看出駭客的動機與技術層次。例如，使用勒索病毒或虛擬加密貨幣挖礦程式代表歹徒的目的是為了賺錢；使用能夠清除或破壞資料的惡意程式，代表他們的動機是為了搞破壞；而使用後門程式或資訊竊取程式，則意味著歹徒是為了從事間諜活動。在技術層次方面，如果駭客使用的是客製化惡意程式，那意味著他們很可能是箇中高手，或者非常了解受害目標的環境。但如果使用的是一般現成的惡意程式，那他們很可能就只是業餘等級，但這也並非絕對。

此外，系統上所發現的惡意程式也可提供線索來了解受害者的環境及網路資安情況，我們可從某個環境所感染的惡意程式來推斷其資安措施有哪些不足之處。例如，若感染的是專門攻擊系統漏洞的惡意程式，那可能意味著端點裝置未套用修補更新；如果感染的是病毒，那很可能是之前的感染並未徹底清除，有些裝置還含有病毒而沒被發現。

本文根據我們 2020 年蒐集的資料來分析 ICS 環境所遭遇的惡意程式威脅，希望能協助企業了解今日 IT/OT 環境在 ICS 資安方面的現況，以及駭客在滲透這些環境之後會做些什麼，此外，也提供一些有關保護這類環境的資安建議。

高階主管摘要：研究發現

1. 勒索病毒依然是全球 ICS 端點一項令人擔憂且快速演進的威脅，一些主要的勒索病毒家族都會攻擊 ICS 端點，美國是受到這類攻擊最嚴重的國家。
2. 虛擬加密貨幣挖礦程式大多經由未修補的作業系統漏洞駭入 ICS 端點，由於 ICS 端點仍然存在著未修補的 EternalBlue 漏洞，因此專門攻擊此漏洞的 Equation Group¹ 工具所散播的挖礦程式在許多國家都相當猖獗，尤其是印度。
3. Conficker 惡意程式仍可在一些作業系統較新的 ICS 端點上散播，即使在已經修補了 MS08-067 漏洞的 ICS 端點上，Conficker 仍可以經由暴力登入方式來駭入系統共用資料夾，進而感染裝置 (該漏洞是 Conficker 會攻擊的一個 Windows Server Service 漏洞)。
4. 一些存在已久的惡意程式在 IT/OT 網路環境依然猖獗，像 Autorun、Gamarue 和 Palevo 這類老舊的惡意程式和蠕蟲會經由隨身碟散布，因此仍經常可以在 ICS 端點上偵測到。
5. ICS 端點上偵測到的惡意程式種類會因國家而異，在十大國家當中，ICS 端點感染惡意程式及灰色軟體的比例最高的是中國，最低的是日本。如前面提到，美國感染勒索病毒的情況最嚴重，印度感染最多的則是挖礦程式。

定義與資訊揭露

IT/OT 網路

這裡指的是 IT 與 OT 網路的匯流，也就是 IT 面的業務流程與 OT 面的實體流程互相連結，這樣的連結使得資料能夠交換，同時也能從 IT 網路監視及控制作業流程。本研究的資料來自於 IT/OT 網路上的 ICS 端點，因此並不包含獨立未連網或不具備網際網路連線的 ICS 端點。

ICS 端點

IT/OT 網路上含有一些工業流程的設計、監視和控制所會用到的 ICS 端點，這些 ICS 端點會安裝特定的軟體來執行一些重要的 ICS 功能，這些軟體包括：

- 工業自動化套裝軟體：例如 Siemens 的 Totally Integrated Automation、Kepware 的 KEPServerEX，以及 Rockwell Automation 的 FactoryTalk。
- 工業工作站 (EWS)：用於工業流程的程式設計，包括：
 - 控制系統 — 如 Mitsubishi Electric 的 MELSEC GX Works 或 Phoenix Contact 的 Nanonavigator。
 - HMI (人機介面) — 如 MELSEC GT Works 或 Schneider 的 GP-PRO EX。
 - 機器人程式設計軟體 — 如 ABB Robotstudio。
 - 設計軟體 — 如 Solidworks。
 - 歷史記錄器 (Historian) 軟體 — 如 Honeywell 的 Uniformance。
 - 監控與資料擷取 (SCADA) 軟體 — 如 Siemens 的 Simatic WinCC SCADA。
 - 現場裝置管理與組態設定軟體 — 如 PACTware 和 Honeywell 的 EZconfig。
 - 序列對 USB 轉接器 — 如 Moxa Uport。

這些 ICS 端點分散於 IT/OT 網路架構上的流程與控制層之外的各個層次，這些 ICS 端點幾乎全都採用 Windows 作業系統。

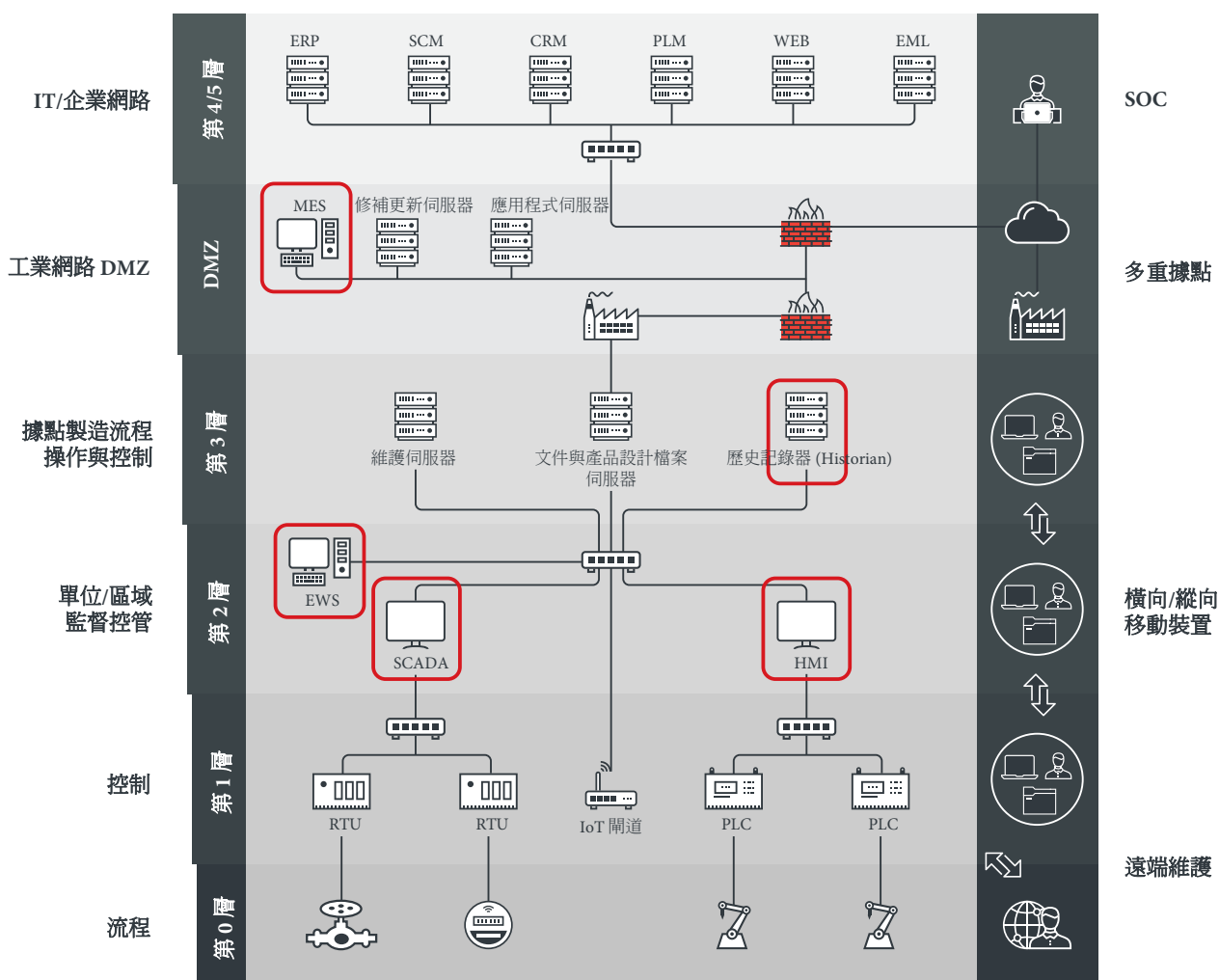


圖 1：Purdue 模型架構中的 ICS 端點 (框起來部分)。

雖然我們知道這些端點上都安裝了 ICS 軟體，但卻無法確定它們是否位於真實的工業流程環境，有些端點可能是用於教育訓練或測試用途，不過我們已經過濾掉一些明顯用來測試的裝置，還有滲透測試人員使用的端點，以及位於大專院校的端點。因此我們可以很肯定的說，我們的資料絕大多數都來自真正的 ICS 環境，且惡意程式偵測資料並未包含滲透測試人員、研究人員或學生用的電腦。

資訊揭露

我們會透過多項不同的資訊來辨識 ICS 端點，例如趨勢科技 Smart Protection Network (SPN) 全球威脅情報網所收到的檔案名稱、檔案路徑及處理程序名稱。相關資料的處理程序也都完全遵照趨勢科技內部的資料蒐集揭露政策來執行，客戶資料在整個過程當中都已匿名處理。

若使用者不希望被蒐集資料，可從產品的管理主控台上關閉認證安全軟體服務 (Certified Safe Software Service)、智慧掃描 (Smart Scan) 以及行為監控 (Behavior Monitoring) 等功能，不過這樣就無法獲得 Smart Protection Network 最新、最即時的威脅防護。

請注意，這些偵測數據是來自我們 SPN 遍布於全球的感測器，因此會受限於 SPN 的涵蓋率，而區域排行及各項數字也會受到我們的市占率影響。

執行 ICS 軟體的端點所面臨的惡意程式威脅

駭客入侵導致的勒索病毒

我們發現針對 ICS 的勒索病毒活動在 2020 年大幅增加，絕大部分是因為 9 月至 12 月期間 Nefilim、Ryuk、Lockbit 和 Sodinokibi 的攻擊數量變多所致，這幾個勒索病毒加起來就占了 2020 年 ICS 勒索病毒攻擊的一半以上。

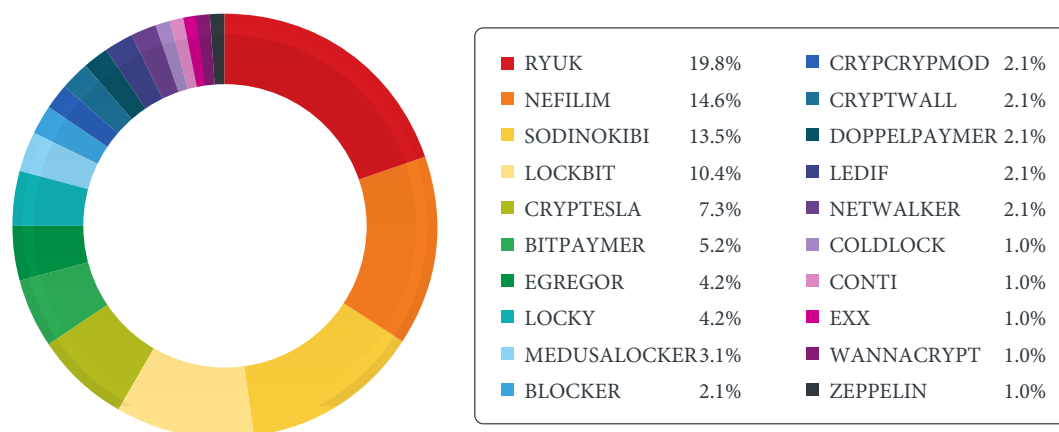


圖 2：2020 年攻擊工業控制系統 (ICS) 的勒索病毒。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

美國是目前 ICS 勒索病毒偵測數量最多的國家，遠遠超過排名第二的印度、台灣和西班牙。

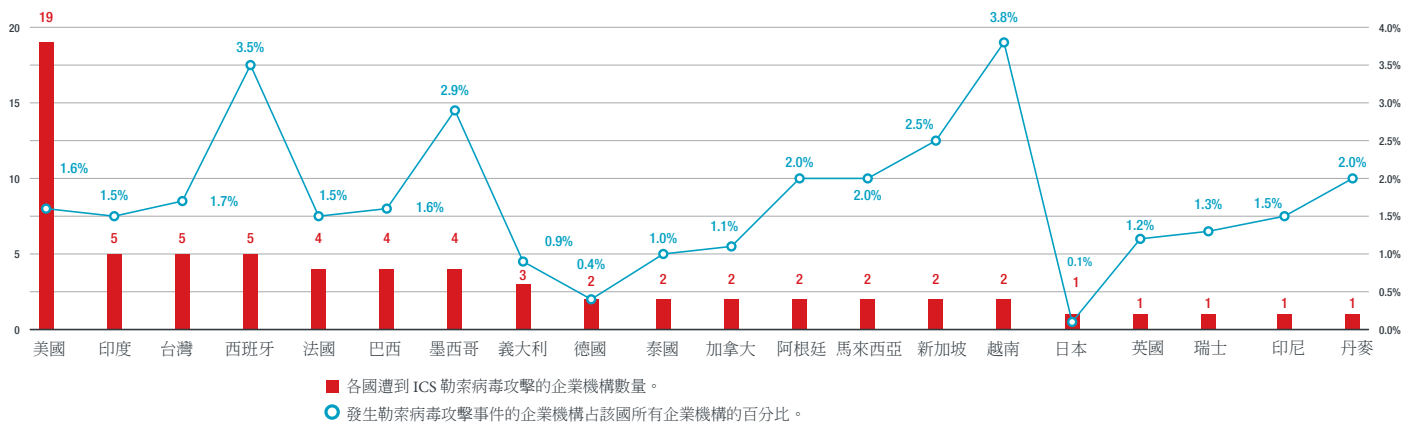


圖 3：2020 年各國偵測到 ICS 勒索病毒的企業機構。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

美國是個大國，因此可能遭到勒索病毒侵襲的企業機構數量龐大。但如果看擁有工業控制系統的企業機構當中有多少比例遭到 ICS 勒索病毒攻擊，那麼其實排行前三名的是：越南、西班牙和墨西哥。

有趣的是，越南的勒索病毒偵測數量應該是 Gandcrab 所遺留下來的效應，此勒索病毒曾經在 2018 年攻擊越南²，但之後大致上已經消失，原因很可能是幕後集團在 2020 年遭到逮捕³。

ICS 勒索病毒可能造成企業無法控制或查看其實體流程，因為像 HMI 和 EWS 這類監控介面都需要根據其組態設定檔以及廠房配置圖的影像檔 (.jpg、.bmp、.png) 來產生監控介面。但是當遭到勒索病毒攻擊時，包括組態設定檔和影像檔的資料都會遭到加密，使得 ICS 軟體無法讀取這些檔案，所以勒索病毒攻擊基本上會讓 HMI 和 EWS 都癱瘓⁴。

如此一來，就會造成工廠的生產力與營業損失，事實上，根據我們模擬工廠誘捕環境的實際經驗⁵，我們每次遇到勒索病毒攻擊事件，大約都需要幾天的時間才能讓工廠恢復正常運作。這是因為 ICS 勒索病毒會造成工業流程變得無法監視與控制。

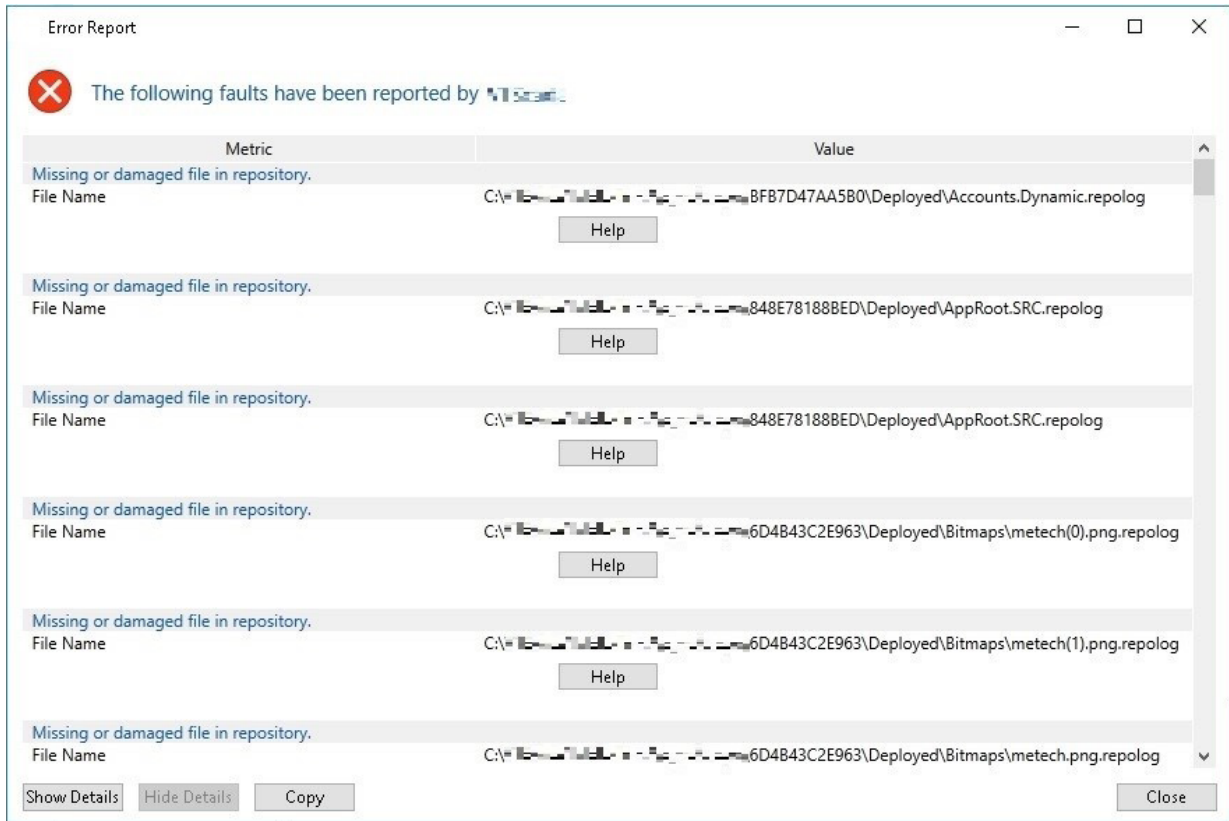


圖 4：HMI 因為其用到的組態設定檔及影像檔遭到勒索病毒加密而無法載入畫面。

圖片來源：趨勢科技。

勒索病毒攻擊對 ICS 的另一項衝擊是最近流行的所謂「雙重勒索」⁷，也就是：受害者的檔案不僅遭到加密，而且還會遭到外流或公開，這對於用來設計或開發工業流程的 ICS 端點尤其是嚴重的威脅。因為 EWS 上所保存的設計圖、程式、文件等等 (如供應商名單、零件清單、獨家配方) 萬一遭到外流或落入不肖之徒手中，駭客將擁有企業的機密資訊或產品設計圖。例如，Sodinokibi 勒索病毒集團就入侵了 Apple 供應商 Quanta 並威脅要公開他們所竊取到的一些文件，這些文件據稱含有最新的 iMac 和 Macbook Air 設計圖⁸。

挖礦程式

除了勒索病毒之外，另一種以賺錢為目標的 ICS 惡意程式是虛擬加密貨幣挖礦程式。雖然挖礦程式不會破壞檔案或資料，但挖礦作業會占用大量 CPU 資源，嚴重影響 ICS 端點的效能。根據我們模擬誘捕環境的經驗⁹，當我們的 ICS 端點遭駭客植入挖礦程式之後，整台電腦都變得很慢。所以，挖礦程式會造成企業無法控制或查看 ICS 端點，尤其若端點本身的 CPU 就不是很強，或者使用的是老舊作業系統，而在工業環境當中，這樣的系統其實相當普遍。

2020 年最猖獗的挖礦程式家族是 MALXMR，這是一個因駭客入侵而導致的挖礦程式，通常是經由無檔案方式安裝到系統上，不過我們自 2019 年起便開始發現一些特殊的 MALXMR 感染案例，這些案例是使用 Equation Group 的工具來攻擊 EternalBlue 漏洞進而在網路內散布挖礦程式並橫向移動。

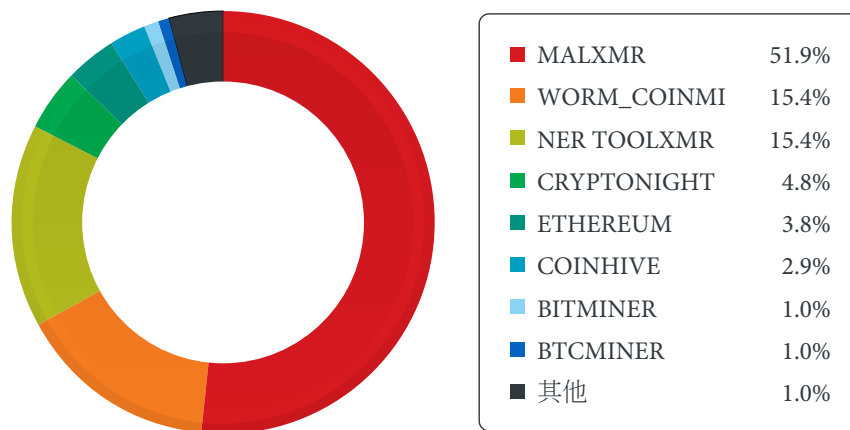


圖 5：2020 年攻擊工業控制系統的挖礦程式。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

在 ICS 端點感染 MALXMR 的國家中，印度就占了所有偵測案例的三分之一以上，但這並不表示印度是 MALXMR 集團主要鎖定的目標。如果看一下 WannaCry 勒索病毒的感染數據就會發現，印度同樣也囊括了 ICS 端點裝置 WannaCry 感染案例的三分之一以上。

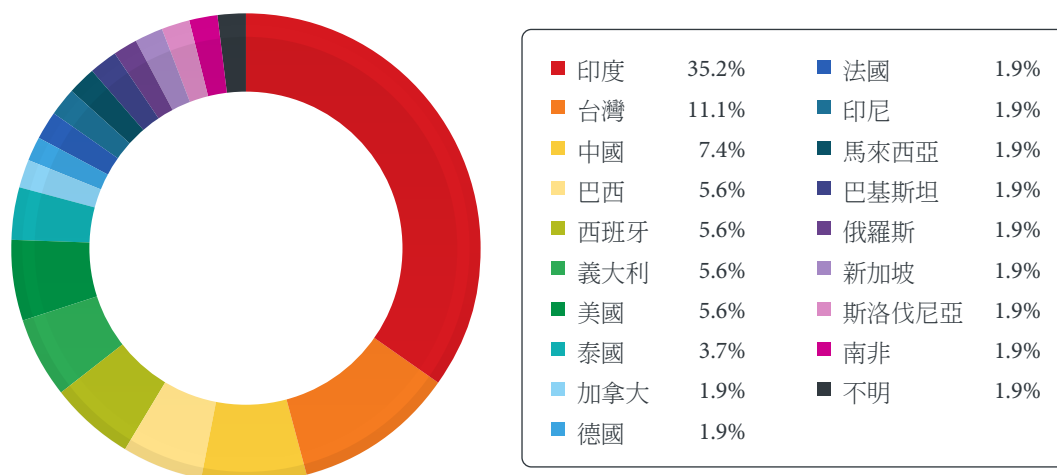


圖 6：各國企業機構 MALXMR 感染案例所占的比例。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

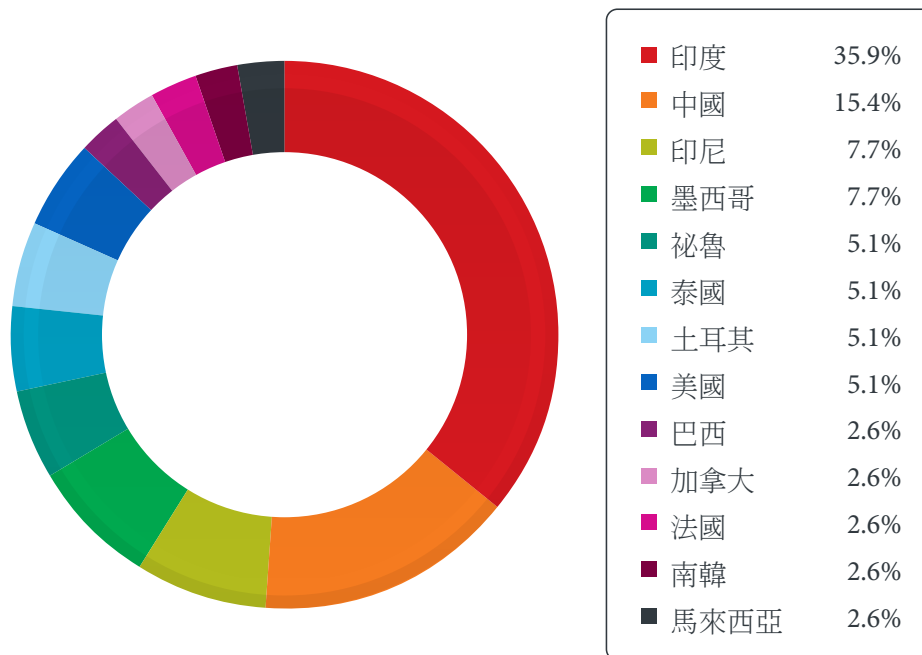


圖 7：各國企業機構 WannaCry 感染案例所占的比例。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

所以，這表示印度之所以成為感染 MALXMR 最多的地方，是因為他們有很多使用 ICS 軟體的電腦都含有尚未修補的 EternalBlue 漏洞，因為 MALXMR 和 WannaCry 皆用到 Equation Group 的工具，而這些工具就是利用這個漏洞。所以從這項資料就能看出，一個國家整體的修補更新套用情形會影響到它是否容易遭到某些威脅攻擊。

Conficker

如同我們之前一份針對製造業環境的研究所發現¹⁰，目前 Conficker (亦稱 Downad) 依舊是 ICS 端點的一大威脅，我們至今仍可在 200 個非重複的端點上偵測到這個最早在 2008 年被發現的電腦蠕蟲。

根據我們的資料，我們所分析到的端點當中至少有 94% 是採用 Windows 10 和 Windows 7 作業系統。而 Conficker 最廣為人知的散布方式就是經由 MS08-067 漏洞，此漏洞讓駭客可利用一個特製的遠端程序呼叫 (RPC) 請求就能從遠端在收到請求的系統上執行程式碼¹¹。然而 Windows 10 和 Windows 7 並不受 MS08-067 漏洞影響，因此我們認為這些感染案例應該是經由隨身碟或是透過字典攻擊方式暴力登入系統共用資料夾 (ADMIN\$) 所致。

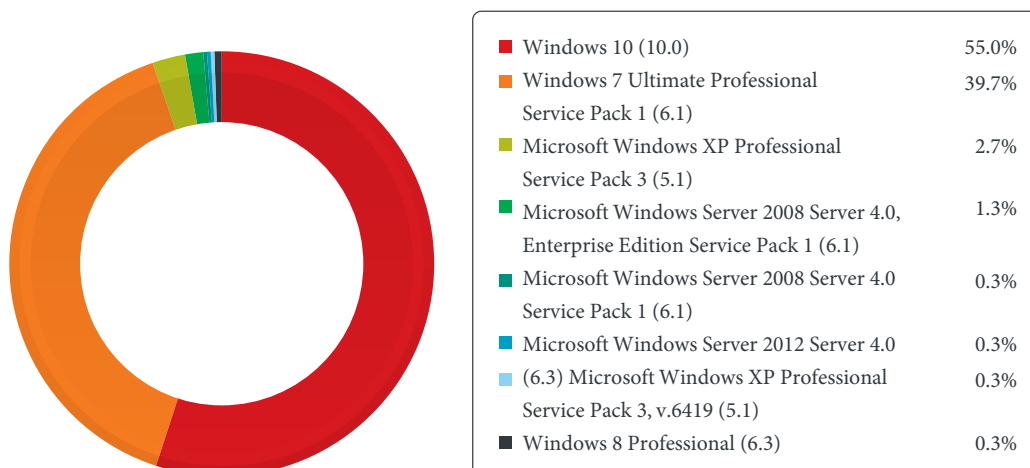


圖 8：偵測到 Conficker 的 ICS 端點裝置作業系統。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

針對前面的假設，我們發現至少 85% 的 Conficker 偵測案例都是來自隨身碟；另外，至少有 12% 的偵測案例是只有在 Windows 系統目錄中偵測到。這表示即使作業系統不存在著 MS08-067 漏洞，Conficker 還是有辦法造成感染。趨勢科技將絕大多數在 Windows 系統資料夾發現的蠕蟲命名為「WORM_DOWNAD.EZ」與「WORM_DOWNAD.AD」（詳細資料請參閱本報告最後「入侵指標資料」一節）。這些算是 Conficker 的特化變種，它們會使用已登入使用者的登入憑證或使用一些常見的密碼來發動字典攻擊¹²，然後將自己複製到「ADMIN\$\system32」資料夾上。這是一項值得注意的發現，因為這意味著即使端點裝置使用的是不受 MS08-067 漏洞影響的新版 Windows 作業系統，還是可能因為系統管理員的登入憑證強度不足而感染 Downad。



圖 9：Conficker 偵測案例的檔案路徑位置。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

蠕蟲感染是一項很難控制的疫情，而像這樣具備多重感染途徑（網路攻擊、隨身碟、暴力登入）的蠕蟲，將使得清除的工作難上加難，資安人員必須確定涵蓋到所有可能的感染途徑。在這樣的情況下，套用系統修補更新（或虛擬修補）、掃描隨身碟上的惡意程式、保護網路共用資料夾、建置入侵防護（IDS 或 IPS）來偵測並防範暴力登入攻擊，都是必要的措施。

老舊惡意程式

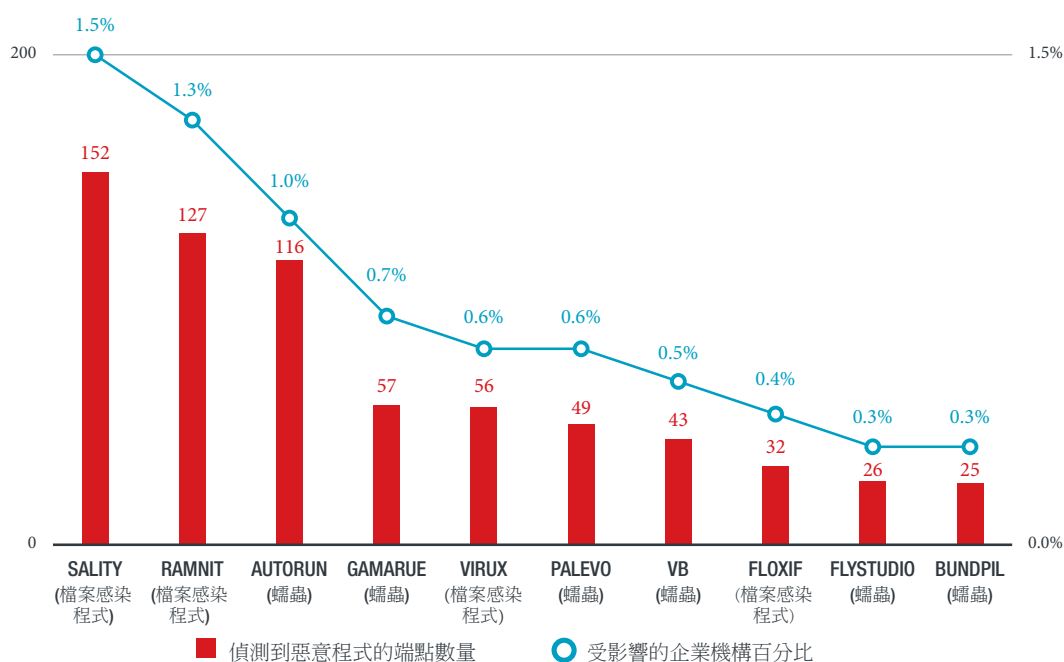


圖 10：ICS 端點上偵測到的老舊惡意程式。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

我們在 ICS 所在的網路中偵測到一些老舊的惡意程式，它們的主要感染途徑是經由網路共用資料夾或 USB 隨身碟。即使這些老舊惡意程式只在不到 2% 的企業機構中出現，但它們的偵測事件卻經常發生，而且經常集中在同一網路某些端點上，代表這是局部性的疫情。

像 Autorun、Gamarue、Palevo 這樣的蠕蟲在 2013 和 2014 年曾經相當猖獗，但隨著今日企業大多已經強迫停用了隨身碟的 AutoRun 自動執行機制（此機制會在隨身碟插入電腦時自動執行「autorun.inf」檔案中指定的執行檔），這些蠕蟲早已不再流行。雖然我們並不訝異在 IT/OT 環境中發現這些老舊的蠕蟲，但企業有些作法卻是導致此狀況的元凶，因此值得注意。首先，使用 USB 隨身碟在不相連的網路之間傳輸檔案和資料確實相當方便，但卻也讓這類老舊蠕蟲有機會擴散。其次，資產設備擁有者若在製作系統備份或建立待機電腦映像時將資料儲存在隨身碟上，但卻未對隨身碟進行資安掃描，很可能會因此連惡意軟體一起備份。

同樣的情況也適用於 ICS 上發現的一些專門感染檔案的病毒，前述讓蠕蟲得以在未連網電腦上殘存的條件，同樣也造成了 Sality、Ramnit 及 Virut 的感染。這些專門感染檔案的病毒甚至比隨身碟蠕蟲更老，Virut 的某些變種甚至可追溯至 2009 年。

儘管這些老舊的蠕蟲和病毒不一定跟任何網路犯罪集團或國家級駭客攻擊有關，但能在 IT/OT 網路上見到它們，代表企業機構的資安存在著漏洞，還有資料備份與隨身碟管理不善。不僅使得這類病毒更難根除，而且還為老舊惡意程式提供了一個繁殖的溫床，這一點從許多端點裝置都在同一個隨身碟上偵測到數個老舊惡意程式就是最好證明。

這也證明了隨身碟很容易成為 ICS 端點的重大資安破口，而且有些進階惡意程式 (如 Stuxnet) 同樣也會利用隨身碟來攻擊 SCADA 系統¹³。

十大國家惡意程式與灰色軟體偵測數量

本節探討 IT/OT 網路最多的十大國家其 ICS 端點偵測到惡意程式與灰色軟體 (可能有害的應用程式、廣告程式、駭客工具等等) 的百分比。

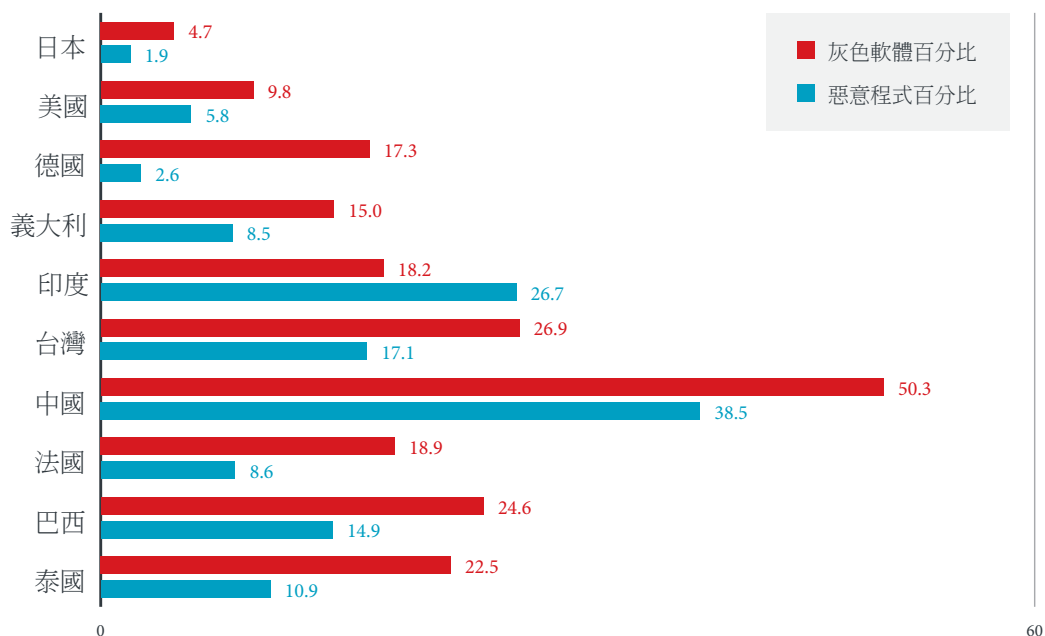


圖 11：十大國家工業控制系統偵測到惡意程式與灰色軟體的百分比。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

上圖顯示，2020 年 ICS 端點偵測到惡意程式或灰色軟體的比例，其中，中國是 IT/OT 網路偵測到惡意程式與灰色軟體最多的國家，日本則是最少的國家。

就地理區域來看，我們可以看到有些類型的威脅在某些國家比較流行。正如前一節提到，美國是感染勒索病毒最嚴重的地區 (參見圖 12，淡紫色部分)。

老舊的惡意程式 (尤其經由隨身碟散布的蠕蟲和專門感染檔案的病毒) 則在印度、中國、美國及台灣最為流行。印度感染挖礦程式、Equated 惡意程式、WannaCry 勒索病毒的情況最嚴重。

日本是感染 Emotet 最多的國家，不過，雖然我們知道 Emotet 在感染系統之後通常還會再植入 Ryuk、Trickbot 或 Qakbot，但在我們的資料裡並沒有看到它安裝了其他惡意程式。德國的 ICS 感染廣告程式的情況最多，最可能的原因是軟體工具內搭了廣告程式。

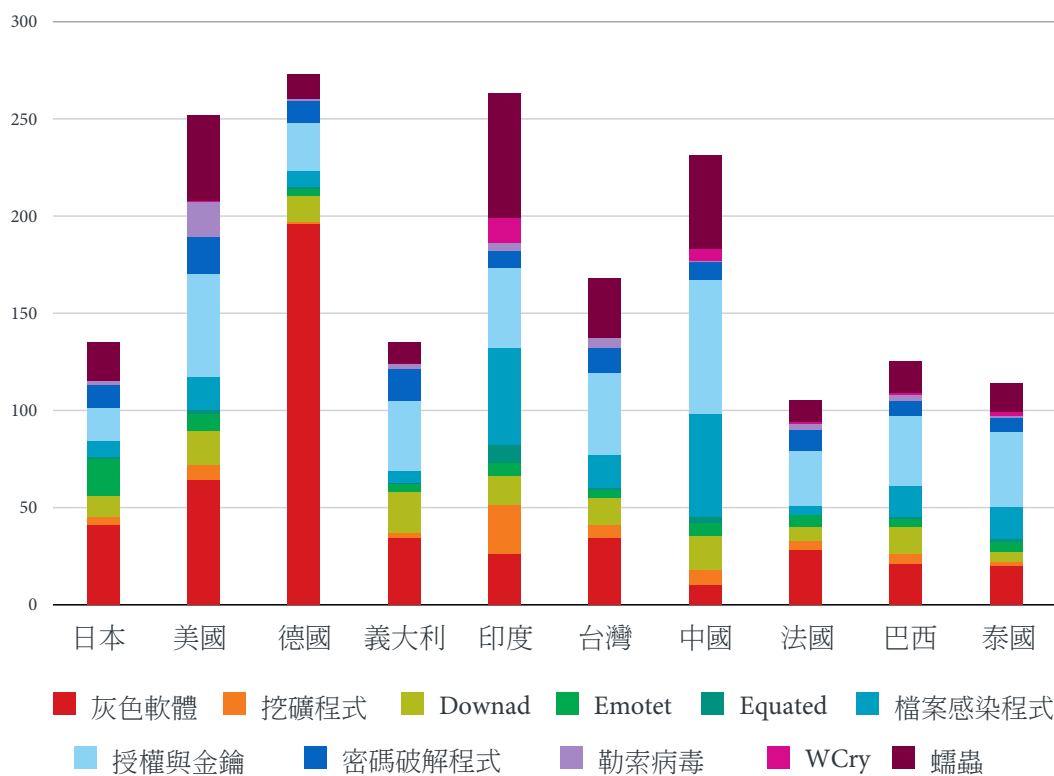


圖 12：十大國家偵測到的惡意程式類型。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

結論

以惡意程式偵測數量來衡量 IT/OT 網路的資安完善度，有助於改進這類網路的資安情況，進而更妥善保護 ICS 端點，防範非預期性停機，避免無法掌握和操控這些端點。

從偵測資料我們可以得出一個結論，不論是現代惡意程式 (如勒索病毒和挖礦程式) 或是老舊惡意程式 (如檔案感染病毒和蠕蟲) 都會感染工業控制系統。換句話說，不論是現代化駭客技巧 (如無檔案惡意程式、就地取材的惡意程式、駭客工具等等)，或是經過千錘百鍊的方法 (舊式網路漏洞攻擊、隨身碟自動執行、網路共用資料夾暴力登入、感染檔案等等) 都能成功感染 ICS 端點。

話雖如此，有些類型的攻擊 (如勒索病毒) 代價很高，企業應小心網路犯罪集團專門「狩獵大型目標¹⁴」的攻擊策略，他們會先搜尋可駭入的目標，找出網路上的關鍵系統來對目標造成最大傷害，進而逼迫受害者就範並乖乖付錢。從過去發生的多起 ICS 勒索病毒攻擊事件即可證明，駭客已經開始覬覦這類系統，並且正積極以它們為攻擊目標。

這意味著，在進行 IT 網路與 OT 網路之間的連結時，應將資安列為優先考量¹⁵，尤其是那些新舊惡意程式都會利用的資安漏洞應優先解決。我們建議 IT 資安團隊在面對 ICS 資安時應先了解工業控制系統的獨特需求，及其系統架構的設計原理。有了這樣的認識之後，接下來，IT 資安團隊應與 OT 工程師共同盤點所有的關鍵系統以及相關的要求，例如作業系統相容性與系統運轉率要求，並了解廠房的作業流程與習慣，進而擬定一套合適的網路資安策略來妥善保護這些重要系統。

建議

以下是有關保護 ICS 端點的一些建議：

- **套用安全修補更新。**儘管這是一項繁瑣的程序，但卻是防止駭客入侵的必要手段。一個最好的例子就是 EternalBlue 漏洞，這個原本是零時差進階惡意程式所用的漏洞，但後來卻已被商品化的 Equation Group 工具用來安裝挖礦程式。每當一種漏洞攻擊手法被公開之後，就會慢慢被其他駭客吸收利用，所以修補系統非常重要。
- **將網路細分成不同網段 (micro-segmentation) 或採用虛擬修補技術。**若無法採用虛擬修補技術，那麼可以將網路細分成不同的網段來限制裝置只能與必要對象進行通訊和存取，進而提升安全。
- **管制網路共用資料夾並強制使用高強度使用者名稱/密碼的組合。**如此可以防止使用者帳號被暴力登入而造成未經授權的存取。
- **採用網路入侵防護系統 (IDS 或 IPS)。**這類系統能標註網路上可能異常的狀況，偵測惡意流量，並提升裝置的可視性。此外，還能分析裝置之間的通訊，建立網路流量的基準，遏止惡意網路活動。有了流量基準與裝置之間的通訊分析，後續就比較容易偵測網路流量是否出現異常現象。
- **安裝惡意程式防護產品。**惡意程式防護產品可清除隨身碟和獨立未連網系統上的老舊病毒和蠕蟲。一些無法安裝資安軟體的獨立未連網 ICS 端點，或是因沒有網際網路連線而無法更新資安軟體的電腦，可使用獨立的惡意程式掃描工具來檢查是否含有惡意程式。
- **設置專門掃描 USB 隨身碟的工作站。**這類工作站可幫那些在獨立未連網系統之間傳輸資料的隨身碟掃描是否含有惡意程式。
- **採取最低授權的原則 (能不開放的權限就不開放)。**OT 網路系統管理員與操作人員應了解一點，操作人員不一定需要 ICS 電腦的系統管理員權限才能操控 ICS，因此可以只提供必要權限讓 ICS 操作人員「使用」這台電腦，但軟體安裝或系統變更的工作還是交由系統管理員負責。

- **考量資安意識與實踐程度的區域性差異。**這一項考量在跨國企業尤其重要，因為這類企業的據點、合作夥伴或分支機構可能遍布全球。最理想的情況當然是所有據點都套用相同等級的安全性，不論據點所在地區的資安意識高或低。
- **盤點並檢查風險忍受度低的系統。**灰色軟體可能造成一些非必要的流量或干擾 ICS 的運作，所以視系統的風險忍受度而定，有些系統即使是灰色軟體也不能容忍。請盤點並檢查所有風險忍受度低的系統，確保它們只安裝已知通過核准的軟體來降低風險。

勒索病毒會對工業控制系統造成嚴重影響，使得企業無法檢視及控制其工業流程，造成工廠營運中斷。工廠內出現勒索病毒，通常是駭客入侵之後的結果(而非原因)。此外，如果在 ICS 端點上發現勒索病毒，意味著系統的存取控管不當，不然就是整個網路已被全面入侵。

我們提供以下兩點建議來解決此問題：

- **採用一份安全清單或「允許名單」。**對於某些特定功能專用的 ICS，或許可以採用一份清單來管制系統可執行的軟體。
- **執行事件應變程序與網路掃描來尋找入侵指標 (IoC)。**勒索病毒集團會經由各種工具及已遭入侵的使用者帳號來存取網路並橫向移動。藉由執行完整的事件應變程序與網路掃描，資安團隊就能判斷駭客入侵的範圍，以及駭客所使用的資安漏洞，然後根據這次的事件來擬定一套更完善的資安策略。

入侵指標資料

Conficker 偵測資料

SHA-256	趨勢科技命名
b2dcad48745325f3176483d698bb544339a052dd	WORM_DOWNAD.EZ
10256bbabf705c32a6ffc2bae5fe78518e722bab	WORM_DOWNAD.AD
5d6e19afa9ea3855a6812a9c28c56019144d672b	
77273bedd01886bc02c27a4b5c7da9d9428256d6	
ffb640274458c125f648b2b9f493a6de61af6329	
ee7276daf5962a3cc58ce87d1ce094d59de0256	
2b8964703209a0bc9606a7d08de3f0d0d2465be9	
7f91223d5e0d6c18ea0214b9dc731ce0739087f2	
c3d4becb6dbf94e948f7a3a81a73507d99a762b4	
85ae9c4e1d513d0f0ed7556c2d51791d7de4e7c0	
0d90356ee974ef47cbaa990c9086a8728e53874f	
71156637cebee20d1b227a591c6819bfe48d12c5	
0a175d05f2803a25d5b8069cdd40c7794743a23b	

參考資料

- 1 Cedric Pernet、Vladimir Kropotov 與 Fyodor Yarochkin。(2019 年 6 月 13 日)。*趨勢科技*。「進階針對性攻擊工具被用於散布虛擬加密貨幣挖礦程式」(Advanced Targeted Attack Tools Found Being Used to Distribute Cryptocurrency Miners)。上次存取時間 2021 年 5 月 14 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/advanced-targeted-attack-tools-used-to-distribute-cryptocurrency-miners/>。
- 2 Viet Nam News。(2019 年 3 月 18 日)。*Viet Nam News*。「網際網路使用者小心勒索病毒攻擊」(Internet users warned of ransomware attacks)。上次存取時間 2021 年 5 月 14 日：<https://vietnamnews.vn/society/507280/internet-users-warned-of-ransomware-attacks.html>。
- 3 Catalin Cimpanu。(2020 年 8 月 3 日)。*ZDNet*。「GandCrab 勒索病毒集團在白俄羅斯遭到逮捕」(GandCrab ransomware distributor arrested in Belarus)。上次存取時間 2021 年 5 月 14 日：<https://www.zdnet.com/article/gandcrab-ransomware-distributor-arrested-in-belarus/>。
- 4 Ryan Flores。(2020 年 12 月 1 日)。*Trend Micro Research*。「現代勒索病毒對製造業網路的衝擊」(The Impact of Modern Ransomware on Manufacturing Networks)。上次存取時間 2021 年 5 月 14 日：https://www.trendmicro.com/en_us/research/20//the-impact-of-modern-ransomware-on-manufacturing-networks.html。
- 5 Stephen Hilt、Federico Maggi、Charles Perine、Lord Remorin、Martin Rösler 與 Rainer Vosseler。(2020 年 1 月 21 日)。*趨勢科技資訊安全新聞*。「捉拿現行犯：運用模擬工廠誘捕環境來捕捉真實威脅」(Caught in the Act: Running a Realistic Factory HoneyPot to Capture Real Threats)。上次存取時間 2021 年 5 月 14 日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot>。
- 6 Ryan Flores。(2020 年 12 月 1 日)。*Trend Micro Research*。「現代勒索病毒對製造業網路的衝擊」(The Impact of Modern Ransomware on Manufacturing Networks)。上次存取時間 2021 年 5 月 14 日：https://www.trendmicro.com/en_us/research/20//the-impact-of-modern-ransomware-on-manufacturing-networks.html。
- 7 Jon Clay。(2021 年 5 月 10 日)。*Trend Micro Research*。「新一波勒索病毒攻擊防範祕訣」(Tips to avoid the new wave of ransomware attacks)。上次存取時間 2021 年 5 月 14 日：https://www.trendmicro.com/en_us/research/21/e/tips-to-avoid-new-wave-ransomware-attacks.html。
- 8 Chaim Gartenberg。(2021 年 4 月 21 日)。*The Verge*。「Apple 遭勒索病毒攻擊造成史無前例的設計圖外洩，歹徒勒索 5 千萬美元」(Apple targeted in \$50 million ransomware attack resulting in unprecedented schematic leaks)。上次存取時間 2021 年 5 月 14 日：<https://www.theverge.com/2021/4/21/22396283/apple-schematics-leak-ransomware-quanta-supplier-leak>。
- 9 Stephen Hilt、Federico Maggi、Charles Perine、Lord Remorin、Martin Rösler 與 Rainer Vosseler。(2020 年 1 月 21 日)。*趨勢科技資訊安全新聞*。「捉拿現行犯：運用模擬工廠誘捕環境來捕捉真實威脅」(Caught in the Act: Running a Realistic Factory HoneyPot to Capture Real Threats)。上次存取時間 2021 年 5 月 14 日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot>。
- 10 Matsukawa Bakuei、Ryan Flores、Vladimir Kropotov 與 Fyodor Yarochkin。(2019 年 4 月 3 日)。*趨勢科技資訊安全新聞*。「工業 4.0 時代製造業環境所面臨的威脅」(Threats to Manufacturing Environments in the Era of Industry 4.0)。上次存取時間 2021 年 5 月 14 日：https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments?_ga=2.209525010.1874680133.1621125958-1328426616.1593403903。
- 11 Microsoft。(2008 年 10 月 23 日)。*Microsoft*。「Microsoft 安全公告 MS08-067 - 重大」(Microsoft Security Bulletin MS08-067 - Critical)。上次存取時間 2021 年 5 月 14 日：<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067>。
- 12 Dan Swinhoe。(2020 年 8 月 5 日)。*CSO*。「什麼是字典攻擊？您如何輕鬆防範」(What is a dictionary attack? And how you can easily stop them)。上次存取時間 2021 年 5 月 14 日：<https://www.csoonline.com/article/3568794/what-is-a-dictionary-attack-and-how-you-can-easily-stop-them.html>。
- 13 Danielle Veluz。(2010 年 10 月 1 日)。*趨勢科技威脅百科 (Threat Encyclopedia)*。「STUXNET 惡意程式攻擊 SCADA 系統」(STUXNET Malware Targets SCADA Systems)。上次存取時間 2021 年 5 月 14 日：<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems>。
- 14 Magno Logan、Erika Mendoza、Ryan Maglaque 與 Nikko Tamaña。(2021 年 2 月 3 日)。*趨勢科技*。「勒索病毒現況：2020 年的兩難問題」(The State of Ransomware: 2020's Catch-22)。上次存取時間 2021 年 5 月 14 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22>。
- 15 趨勢科技。(2020 年 3 月 18 日)。*趨勢科技資訊安全新聞*。「工業物聯網 (IIoT) 威脅：保護連網產業的安全」(The IIoT Threat Landscape: Securing Connected Industries)。上次存取時間 2021 年 5 月 14 日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-iiot-threat-landscape-securing-connected-industries>。



TREND MICRO™ RESEARCH

趨勢科技為網路資安解決方案全球領導廠商，致力建立一個安全的資訊交換世界。

Trend Mico Research 背後擁有一群熱情的專家為後盾，他們熱衷發掘最新威脅、分享重要分析情報、全力為遏止網路犯罪而努力。我們的全球團隊每天都協助客戶偵測數以百萬計的威脅，為業界漏洞研究揭露的先驅，經常發表有關最新威脅偵測技巧的創新研究。我們不斷鑽研並預測最新威脅，發表令人深思的研究。

www.trendmicro.com

