FORCEPOINT
POWERED BY Raytheon

有效預防勒索軟體 CRYPTOLOCKER

FORCEPOINT APX 解決方案

Cryptolocker 是什麼？

Cryptolocker 是一款惡名昭彰的勒索軟體，出現於 2013 年底，到了 2014 年底時在澳大利亞已變成非常活躍且顯著的威脅。

Cryptolocker 是由俄羅斯網路罪犯 Evgeniy Bogachev 開發而來，最初透過 Gameover Zeus 僵屍網路病毒作為傳播途徑，導致全球有超過 23 萬台電腦受到病毒感染。

勒索軟體是一款惡意軟體，企圖透過感染和控制受害者的設備、或者儲存在設備中的檔案或文件，來敲詐勒索電腦使用者以獲得贖金。

一般來說，勒索軟體會透過“鎖住”電腦的方式阻止受害者正常使用，或者透過將電腦上的文件和檔案加密的方式，來阻止使用者存取資料。

Gameover ZeuS 木馬則是一種對等於僵屍網路的病毒，其根源於早前出現的 ZeuS 木馬。該木馬透過使用 Cutwail 僵屍網路而散播開來。

不同於其上一代木馬 ZeuS，Gameover ZeuS 使用加密的對等通信系統進行端點及命令控制伺服器的通訊，從而大大降低了被法律機構偵查的風險。

勒索軟體的歷史

勒索軟體的歷史始於 AIDS，也被稱為 PC Cyborg 木馬，其是替代 AUTOEXEC.BAT 檔的一種木馬病毒。AUTOEXEC.BAT 檔主要被用來記錄電腦啟動的次數。一旦啟動次數達到 90 次，AIDS 將隱藏檔案目錄，並對 C 槽上所有檔案的名稱進行加密（造成系統無法使用），然後要求受害使用者要繳交贖金以重新更新授權，且要透過郵遞的方式聯繫 PC Cyborg 公司來支付 189 美元。

網路駭客會隱藏這些資訊，直到使用者支付贖金，這類敲詐勒索軟體從 2005 年五月開始變得非常猖獗。

到 2006 年中，Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip 和 MayArchive 開始使用更為複雜的 RSA 加密機制，金鑰大小不斷增加，導致破解加密變得更加困難。

2011 年，一種勒索軟體病毒通過模仿 Windows 產品啟動通知介面，導致眾多使用者為這種偽造的啟動而支付費用，同時勒索軟體也成功入侵使用者的 Windows 設備存取資料。

2013 年 7 月，隨著第一個針對 OS X 作業系統的勒索軟體的現身，蘋果公司 OS X 作業系統成為網路駭客攻擊的目標。

到了 2014 年末，在第一個 CryptoLocker 病毒爆發的前兩個月裡，支付的贖金金額已經超過兩千七百萬美元。

Forcepoint® 安全實驗室的研究團隊觀察後發現，勒索軟體在 2014 年已氾濫成災。這種惡意軟體的攻擊在 2015 年也沒有出現任何減緩的跡象。

勒索軟體的類型

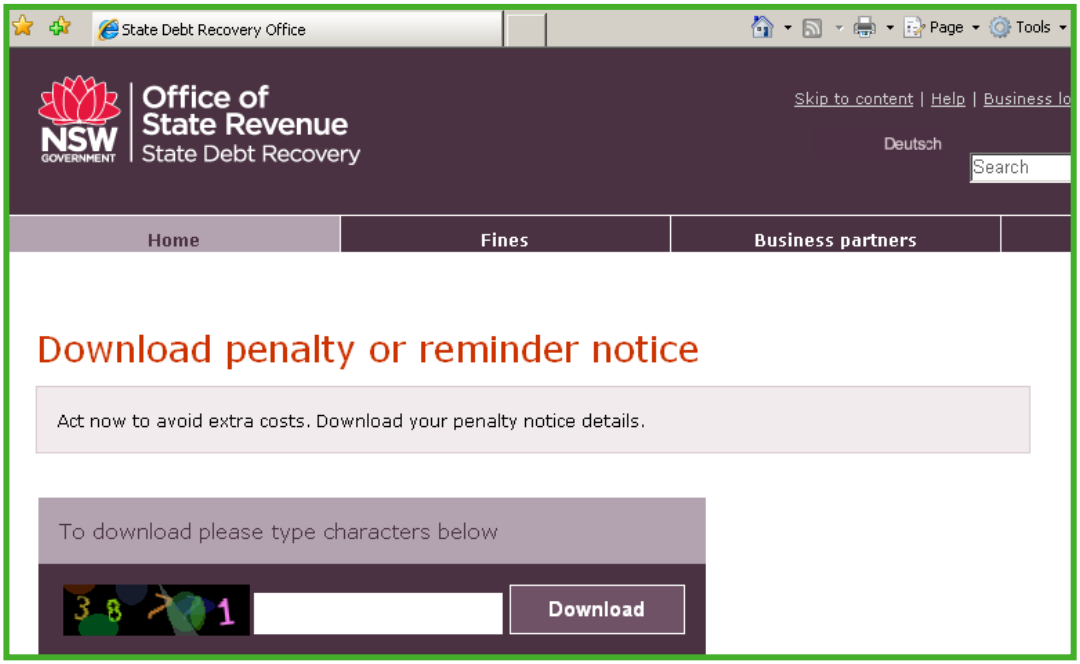
- 鎖住桌面的勒索軟體 - 這類勒索軟體會鎖住電腦的桌面，直到客戶支付贖金給網路駭客後才能恢復正常使用。
- 主要開機磁碟區（MBR）的勒索軟體 - 這類勒索軟體會導致電腦開機啟動停止並被鎖定，直到用戶支付贖金給駭客後，用戶才能正常開機。
- 加密勒索軟體 - 這類勒索軟體透過對資料加密並扣留加密金鑰，以阻止用戶存取資料，直到支付贖金給駭客，系統才恢復正常存取功能。

以澳大利亞為例的勒索軟體

在我們的案例分析中，以澳大利亞為例子的勒索軟體事件出現了從引誘到感染的典型攻擊過程。

勒索軟體經常以電子郵件作為誘餌散播病毒或者透過被入侵的網站（通常為惡意廣告）進行傳播。今天分析的案例以電子郵件為誘餌，電子郵件的主題則是關於測速照相產生的罰單。典型的郵件主題為 “罰單 ID 號碼”-<隨機數字>/測速照相監測。

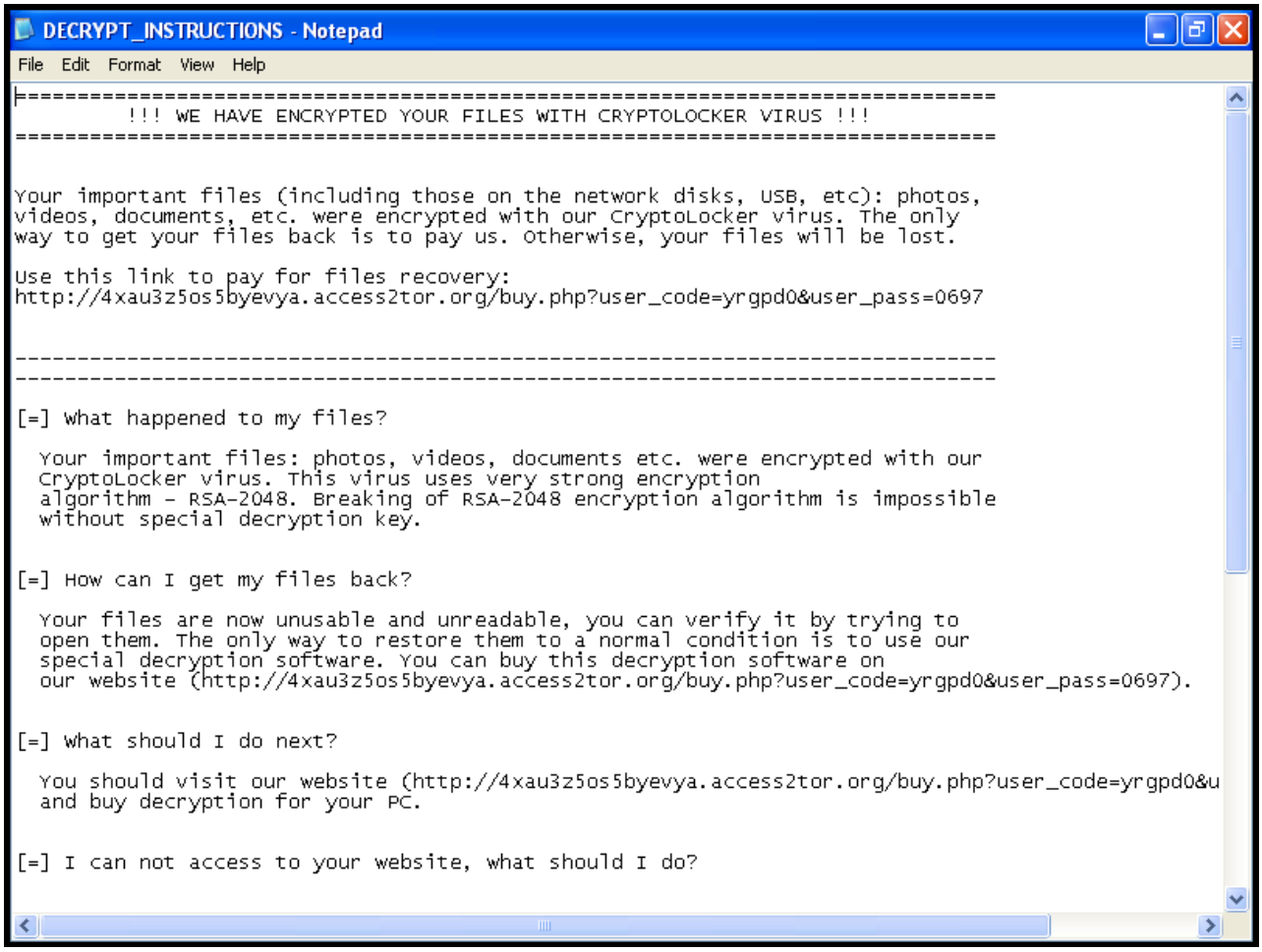
陷阱電子郵件包含一個 URL 連結（在這個案例中是一個被入侵的 wordpress 主機）。使用者被傳送至某個網站的連結且決定採取行動。



在這個案例中，我們看到的是一個來自新南威爾斯州的財政辦公室（OSR）的罰單通知聲明。其網址為 http://www.osr.nsw.gov.au/。為了避免使用者對該財政辦公室是否為合法機構產生懷疑，駭客透過社交工程讓使用者相信並願意執行操作。請注意貌似合法的標識以及 CAPTCHA（驗證碼）的輸入表格，為這個欺詐網站添加了一些合法性，同時網站的介面鼓勵使用者執行進一步的點擊行為。欺詐網站的主機輪番變化，包括 hxxp://nsw.gov.yourpenalty.com/ 和 hxxp://osr.nsw.mypenalty.org/。類似網址的變化在未來很可能還是會出現。

一旦使用者上當受騙點擊進入，將看到如下警告的提示：

透過安裝於使用者設備上的 HTML 檔案提供了解密方式。此時使用者需要連至另一個網站，並被鼓勵執行交易操作。



正如圖片展示的典型案例所示，解密伺服器網站提供兩種解密的價格。如果使用者立刻付款，他們只需要支付 2.4 個比特幣，價值大約 499 美元。如果三天之後付款，使用者需要支付大約 998 美元。

透過計時器的顯示鼓勵使用者立刻付款。惡意網站也顯示被加密的檔案數量。如果使用者不瞭解如何使用比特幣付款，網站還會提供指導說明。

正如我們之前的立場，我們不鼓勵使用者向網路罪犯支付比特幣來解密檔案。比特幣的支付無法保證檔案能夠被成功解密。如果您擔心可能會遇到勒索軟體網站（在攻擊週期的任何一個階段），您可以將該網站網址提交至我們的線上網路安全智能分析工具，網址為 http://csi.websense.com/，其能檢驗這個網站連結的可靠性。

通過不同國家代碼的頂級網域名稱（ccTLDs），Torrentlocker 的週期呈現多樣性變化的特點。我們觀察到 .com, .at（奧地利），.lt（立陶宛）和 .ru（俄羅斯）。這些變化包括如下資訊：

```
hxxp://hochim.ru/wp-
content/themes/thems/readip.php?eid=8335416278221988351634911194654464864426932877911359115391878239578365375

hxxp://kronbichler.at/wp-
content/themes/thems/readip.php?eid=697637427688695726393931299536381275113472867364549258517783237992424632 4

hxxp://zsohajnowka.pl/wp-
```

```
content/thems/readip.php?eid=623534149942711528344994141811459
```

正如白皮書上面所描述的，偽造的州政府財政辦公室網站也經常變化，導致在沒有即時偵測技術的情況下，對網站真偽的偵查變得十分困難。

財務服務部門是這類攻擊最主要的目標對象。

如何避免勒索軟體的入侵

在以澳大利亞為目標的勒索軟體進行攻擊之際，Websense 客戶正因我們先進分類引擎（ACE）的即時分析技術得到有效的防護。在攻擊的不同階段，我們的先進分類引擎（ACE）可以提供不同的保護，詳細內容如下：

- 第二階段（引誘）- ACE 偵測到電子郵件的陷阱及郵件裡面提到的網站。
- 第三階段（重新導向）- ACE 偵測到電子郵件陷阱中的連結，以及偽造網站的最終目的地網站。
- 第五階段（植入惡意檔案）- 如後面檔案沙箱報告中所顯示，ACE 可偵測到被植入惡意程式的檔案。
- 第六階段（回報通訊流量）- ACE 可偵測到命令控制（C&C）的通訊流量，阻止正在運作的惡意程式。

在我們的檔案沙箱報告裡，勒索軟體的有限負載被劃分為惡意。

在本白皮書撰寫之際（2015 年 2 月 25 日），檔案樣本在 Virus Total 上的檢測速率為 57 個，防毒軟體廠商只篩選出 3 個。

當邁入 2016 年，勒索軟體仍持續演變，一旦設備感染病毒，檔案被加密，使用者將無能為力。而為了加強您的企業內外的整體安全，我們建議企業訓練員工對勒索軟體的危險和各種徵兆有更多的察覺，並採用恰當的技術在攻擊生命週期的早期便能進行辨識和防護。

網路攻擊模式 - 對 Kill Chain（威脅殺傷鏈）的理解

進階攻擊的特徵包括一系列階段。透過這些階段，攻擊者逐步獲得組織的存取權限，並進行病毒的散播，最終任意竊取組織的資料。為了更精確地描述不同階段攻擊模式潛在的細微差異，進階攻擊按照如下描述，被劃分為七個階段，也被稱為進階攻擊的 “Kill Chain”（威脅殺傷鏈）。

為了評估組織機構對進階攻擊防禦的有效性，Forcepoint 專業人士將評估企業用戶是否已經建立可涵蓋整個 Kill Chain（威脅殺傷鏈）七個階段在內的完整防禦網。

Forcepoint 核心技術

當前的先進攻擊趨勢更廣為利用 Kill Chain（威脅殺傷鏈）中多種混合手法，已經無法依靠不同且分散的資安廠商來實現“安全的深度”，因威脅情資無法整合聯防而容易形成防護盲點。需要專一的資安廠商，透過智能且情境感知的安全技術而達到有效的安全防護，進而阻止橫跨整個 Kill Chain（威脅殺傷鏈）不同階段的攻擊。

Forcepoint® TRITON® Enterprise

Forcepoint® TRITON® 解決方案可對本地和遠端的員工，針對最新攻擊提供完整的混合式安全防護方案。你可以透過增加 Forcepoint 網路安全智慧（CSI）服務，獲得線上的惡意程式沙箱，並可直接在線上與 Forcepoint 安全實驗室的資安研究員聯絡。

透過所有的 TRITON 解決方案，您可以獲得：

- 統一的架構 - 降低總持有成本（TCO）。
- 完整的網路安全威脅情資 - 共享涵蓋網頁、電子郵件和資料安全的威脅情報。
- 完整的政策和報告 - 簡單且易於使用的單一虛擬管理控制平臺。

無論您位於何處

Forcepoint TruHybrid™提供您全世界最佳的安全部署

能同時保護雲端和本地端的資料安全的優勢 - 通過單一控制平臺實現對整個系統的管理。TruHybrid 部署透過以下方式，解決了核心的網路安全挑戰：

- 提供大容量的軟體及硬體設備，以滿足大型辦公室的需要。
- 使用雲端服務以保護缺乏技術資源的小型衛星型態的辦公室，並提供硬體設備的支援。
- 在雲端環境中保護移動工作者的使用安全，避免移動工作者將流量傳回到企業內的中心區。

TruHybrid 提供具有優勢的電子郵件安全服務：

- 大量寄入企業內的電子郵件在雲端被層層過濾，減少客戶本地端硬體設備承載流量負荷的麻煩。
- Forcepoint V-Series™設備，提供客制化的安全政策、精細的報告和企業級的資料外洩防護（DLP），讓企業能有效執行安全控管措施。

Forcepoint 協助您解決問題

我們的安全解決方案符合嚴格的聯邦安全法規標準。

您面對眾多的資料安全需求，不但需要阻止來自多個攻擊行動，同時還要滿足澳大利亞信號局 - 消除目標式網路入侵控制的戰略。Forcepoint 協助您保護處在各式混合式目標攻擊行動中的資料安全無虞，同時能夠洞察被阻止的惡意活動，並保證符合安全的活動能正常運作。我們的產品和平臺符合聯邦安全法規的嚴格要求及標準，包括 Common Criteria, FIPS 140-2, HSPD#12 和 DOD/Army STIG。此外，Forcepoint 符合美國-防禦部門關於社交媒體使用的需求（瞭解更多）。

- 聯繫我們，取得我們符合安全法規標準和認證的更多資訊。
- 關於我們的資料防護產品。

Forcepoint ACE 先進分類引擎：為什麼沒有任何一家公司比 Forcepoint 能阻止更多的攻擊

ACE（先進分類引擎）內建在 Forcepoint TRITON®架構上的所有產品線，它能向客戶通報即時的安全分析評等，可預知威脅的變化。ACE 是 Forcepoint 的獨家技術，其採用綜合風險評估和預測分析技術，能對 Web、Email、Data 和 Mobile Security 提供 Inline、內容情境感知的即時安全防護，協助企業即時的阻擋威脅。

- 閱讀 ACE 白皮書
- 瀏覽 ACE 網站
- 關於我們的 AP-Web 產品

有效防範零時差威脅和進階持續性滲透攻擊（APT），提供最先進的安全解決方案

大量的攻擊行動，使得包括網路釣魚和專門的惡意軟體等在內的針對性攻擊更有機會肆虐。Forcepoint® TRITON® Sandbox Module™提供更高階的安全技術以防範零時差威脅和進階持續性滲透攻擊（APT），這些威脅可能以網頁或者電子郵件作為管道進行攻擊。組織機構可通過行為式沙箱檢查和可付諸實施的網路釣魚活動報告，在攻擊防護方面變得更加主動與積極。

讓社交媒體的使用變得安全且具效能

社交網站是您維繫工作關係和公眾形象的核心。但是它也會給您帶來風險和負面效應。Forcepoint 能夠確保您的員工安全地使用社交網站，且為工作創造生產效能。

- 下載我們的免費社交媒體可接受使用策略（AUP）工具包，並將該工具包用在您的組織機構中。
- 瞭解 Forcepoint 如何在社交網站上保護您的組織機構和員工。
- 瞭解 Forcepoint 如何和 Facebook 合作，讓使用者免受惡意連結的攻擊。