

來自荷蘭 RedSocks Security

惡意威脅早期預警解決方案

許多公司面對惡意程式以及進階持續性滲透攻擊(APT)的防護時，總有著不足或不正確的資安觀念。多數人認為只要在網路架構好防火牆，並在用戶端安裝了防毒軟體就可以簡單的解決公司外部的資安威脅或是電腦病毒問題。不過現在的惡意程式已經跟以前不一樣了，基本的防護已經無法解決日新月異的電腦病毒以及駭客攻擊。在過去的統計中發現平均需要187天，公司或組織才會發現被惡意程式入侵，或是中了電腦病毒，無形之中受到了極大的損害。

越來越多的資安專家認為，以前的病毒防護方式或者網路攔截模式已經無法阻止現今的資安威脅。現今的社會，資安威脅可以透過非常多種不同的形態進入公司或組織的系統或資料庫，例如無線網路、VPN虛擬網路、同事們自己攜帶的設備，像是手機、平板或是行動網路等外部存取裝置。這表示基本的資安防護已經抵擋不了現今的資安威脅，各種用戶端的使用習慣，使其能透過更多管道進入公司或組織內部。所以企業或組織不能放任資安威脅在內部遊走，應該要採取跟過去不同的做法，並投入更積極的資安防護模式來對抗現今的惡意威脅。

風險控管的訣竅，就是在發覺應對、預防、偵測三者之間取得平衡

以過去的經驗法則進行資訊安全防護，已經無法有效地對付現今惡意程式以及資安威脅，今日的惡意程式已經能夠巧妙的避開防毒軟體或是繞過企業的防火牆架構。所以一個有效率並且即時的防護機制，讓您能夠在資安威脅發生的時候；甚至在發生之前，做出適當的防護應對，得以讓資安威脅所產生的風險降到最低。

獨家設計

身為The Hague Security Delta的合作夥伴，RedSocks Security研發獨家偵測和對抗惡意軟體的概念，自2012年以來，已經革新許多檢測惡意威脅的解決方案，促進企業不受病毒威脅得以持續發展。RedSocks Security藉由提供人工智慧、機器學習和網路威脅情報的蒐集，以持續的網路監控作為解決方案，並提供即時的警報，讓您能夠立即回應威脅。

強大而持續性攻擊時的回應模式

檢測方式採用精準而非透過大量警訊模式，RedSocks的防護方式是建立在解決進階持續性滲透威脅(APT)的基礎上。一旦被進階持續性滲透威脅(APT)攻擊，用戶端設備的網路行為就會產生異常的變化，RedSocks會發出警報，並通知哪些用戶端設備可能會遭受感染，或是哪些已經被感染。它會對可能被感染的設備進行驗證，並密切監控且對任何可疑的惡意活動發出警報。

RedSocks惡意威脅智慧團隊

RedSocks惡意威脅智慧團隊是由一群經驗豐富的資安專家組成，利用已知以及新興的演算法研發出一套獨家的規則。持續監控成千上萬的僵屍網路，自動分析超過35萬件惡意軟體的行為和目的。這些訊息不斷地被蒐集到RedSocks的設備中，從而讓使用者受到最佳的保護，抵禦最新型病毒的威脅。

為何選擇 RedSocks 安全解決方案

- 非侵入式的網路安全監控，保護來自雙方的隱私以及資訊安全。
- 不間斷的網路安全監控，隨時提醒您企業組織內部的資安威脅突發事件。
- 完整保留所有惡意程式或資安威脅行為，以利後續惡意行為分析。
- 縱觀企業組織的網路環境架構，從中發現資安威脅的盲點，或是潛在的危機。

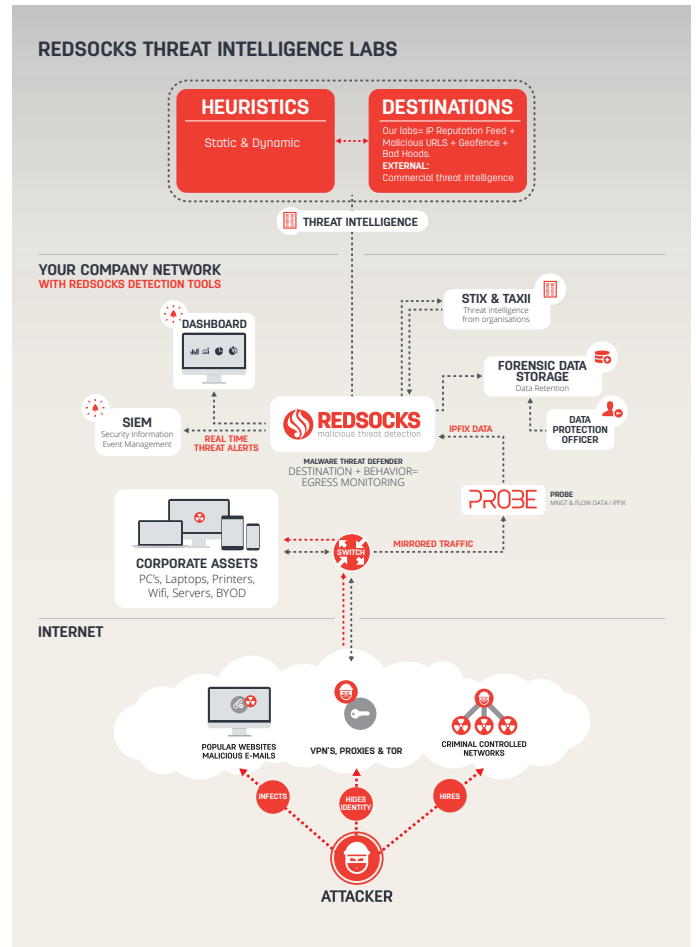
這是怎麼做到的？

RedSocks安全解決方案的設計是一種非侵入式即可達到防護的一種架構，它能即時監控網路封包，並即時發現可能潛在的惡意威脅是否對外送機密資料。

對RedSocks而言，保護客戶的資料安全和企業隱私是我們最重視的部分。因此我們的整個系統、惡意威脅檢測器(MTD)和網路監測裝置(Probe)，都是根據這一項理念而設計。

RedSocks網路監測裝置(Probe)能夠完整存取網路封包的裝置，是設計成以點對點的方式送往至RedSocks惡意威脅檢測器(MTD)進行分析，例如：對於時間校時功能其實無須指定任何外部網際網路連線，也不需要額外追加儲存媒體。惡意威脅檢測器(MTD)也提供了鑑識資料存儲服務給應用程式分析以及網路封包採集器。同時惡意威脅檢測器(MTD)也支援使用了資料封包傳輸層安全性協定(DTLS)的通道加密傳輸機制，並確保第三方服務進行的傳輸能夠得到更安全的保障。

我們把焦點放在網路封包的Meta-data(或稱Flow-data)，能夠長期提供更快速的分析，以利檢測更複雜的惡意程式、進階持續性滲透攻擊(APT)或是其他惡意行為。由於MTD僅專注在分析封包的Meta-data，而不是資料本身的內容，所以也不必擔心機密資料外流。Probe / MTD 的架構不會傳送多餘的流量，並且不設定從中攔截機制(Man-in-the-middle)，所以不會增加網路環境中的負擔。所以使用此裝置不會對網路與系統架構的效能與可靠度造成影響。以上這些獨特功能使得RedSocks Security的解決方案能夠兼具安全性並保有網路的隱私性。



RedSocks 安全解決方案與一般資料保護法規 (GDPR)

歐盟一般資料保護法規為個資隱私及安全性建立了一套新的標準，這也影響公司蒐集與處理個資的作業方式，一般資料保護法規的範圍遍及歐盟境內相關的業務，以及儲存在歐盟境內的資料。若是未遵循GDPR將會面臨巨額罰金，最高將處以全球營業額的 4%或是 2,000 萬歐元的罰金。且GDPR不僅要求公司必須遵循個資規定，若是發生個資外洩也必須在72小時內通報資料保護主管機關。要同時兼顧資訊安全與個資法規不是一件容易的事。當使用RedSocks惡意威脅檢測技術時，若資訊網路基礎架構中的資料發生外洩，RedSocks的資安防護措施能夠被有效的操作以追蹤並提供相關的鑑識證據。

想要獲得更多資訊，可以透過以下信箱帳號跟我們聯繫 Sales@cyberview.com.tw



<http://www.cyberview.com.tw/>