今年最需要關注的網路安全趨勢是什麼？

Reported: Jason
Date: Oct. 8th 2019

Introduction

AENEAS

2018年各類網路安全事件頻繁出現，隨著新出現的網路威脅攻擊浮出水面，新的APT集團現身，以及圍繞數據隱私的更多規定，2019年將是網路安全領域的又一個重要年份。以下是2019年最值得關注的網路安全趨勢。

更多漏洞

AENEAS

研究人員在2018年發現了兩個關鍵的Apache Struts 漏洞之後，他們認為很快就會出現，另一個重大漏洞，這個漏洞源於該軟體的缺陷，它一直是Equifax漏洞的核心。

「Apache Struts提出了一個獨特的挑戰，因為它被許多其他面向網路的程序所包含，這意味著傳統的漏洞掃描程序可能無法檢測到Apache Struts，但僵屍網路掃描漏洞將會發現它。」

2018年伊始，兩款基於硬體的側通道漏洞——Spectre和Meltdown被曝光，引發了軒然大波。這影響了過去10年在電腦和行動設備上，廣泛使用的微處理器，包括那些運行Android、Chrome、iOS、Linux、macOS和Windows的微處理器。

安全專家預測，Spectre變種將在2019年繼續被發現。

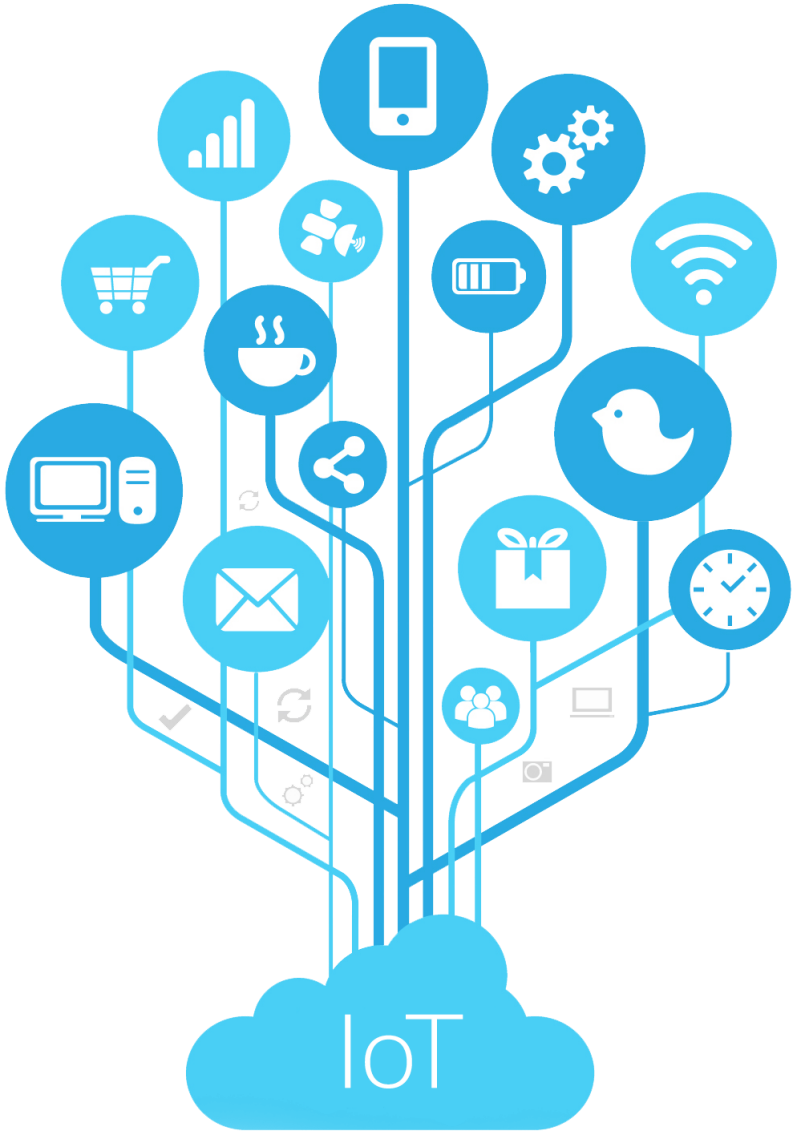
複雜的物聯網攻擊

AENEAS

物聯網（IoT）市場爆發……

但許多此類設備的製造，很少、甚至沒有考慮到安全問題。自2016年Mirai僵屍網路出現以來，研究人員已經看到物聯網設備，被惡意利用來發動一系列威脅性攻擊，包括加密、勒索軟體和行動惡意軟體攻擊。

未來形勢可能會更加糟糕：「到2019年，物聯網威脅將變得越來越複雜，從僵屍網路和游離的勒索軟體感染，發展到到APT監控、從而進行數據過濾，直接操縱現實世界，以擾亂運營。」



勒索軟體又回來了

AENEAS

當涉及到網路威脅時，專家預計加密（攻擊）會從網路上消失，勒索軟體也會回到一線。

對許多網路罪犯來說，加密攻擊並不像他們最初希望的那樣有利可圖，事實證明，只有當攻擊者能夠感染數萬，或數十萬台設備時，他們才能賺錢。

然而，勒索軟體仍然有利可圖：「例如，SamSam已經從贖金軟體攻擊中，賺取了近600萬美元。」

技術人員說:

我們已經開始看到，新的勒索軟體變種複製這種模式，

不希望看到新的一批勒索軟體家族，繼續擴展這種攻擊方法。

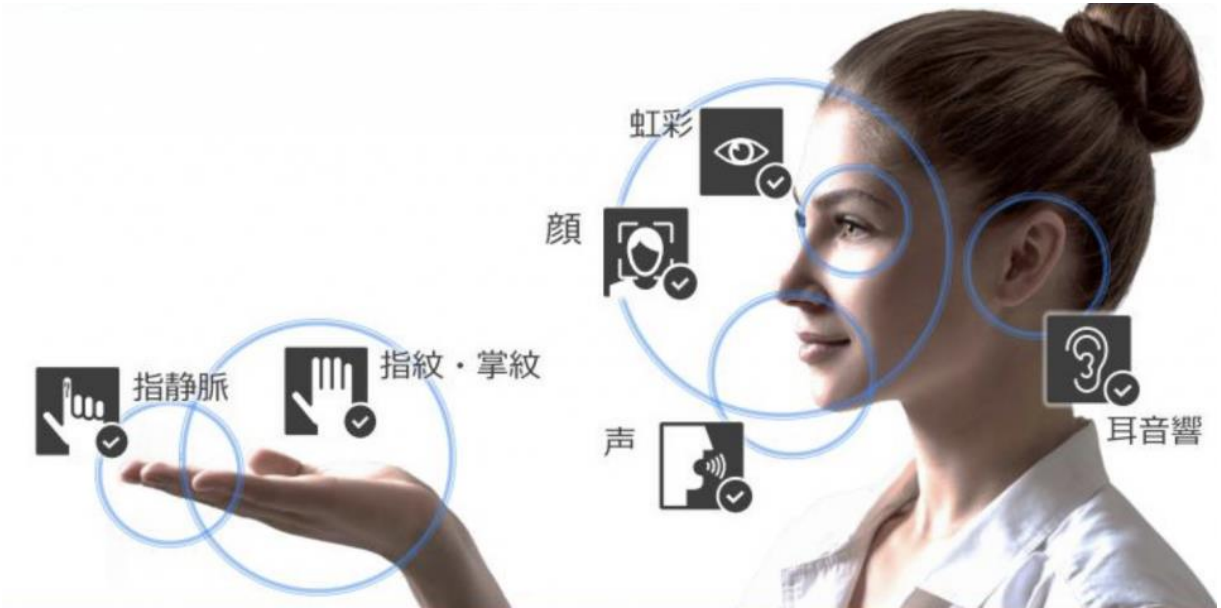
不安全的生物辨識技術

AENEAS

生物辨識技術已經成為2018年，銀行和其他機構進行人員身份驗證的首選方法。

然而，2019年將可能會發生更多，與生物辨識系統相關的安全事件。

卡巴斯基實驗室的研究人員表示：「已經發生了幾起重大的生物辨識數據洩露事件。」



供應鏈攻擊

AENEAS

在2019年「我們將看到網路犯罪分子，繼續專注於攻擊關鍵的軟體供應鏈基礎設施，以實施更大規模的攻擊。」

攻擊者已經開始認識到，供應鏈攻擊的優勢——從2017年6月的NotPetya 活動開始，隨後迅速蔓延，從全球數千台電腦上清除數據。2018年發生了大量針對供應鏈的攻擊，涉及達美航空（Delta Airlines）和百思買（Best Buy）等公司。

更加快速的漏洞修補

AENEAS

隨著漏洞補丁在2018年成為人們關注的焦點，

圍繞漏洞披露過程的敘事，也從披露時的90天準則，演變為更即時地發佈補丁。

「由於供應商越來越重視漏洞——無論是透過錯誤賞金計劃，變異分析或測試，從 發現 >> 修補 >> 公開 所需的時間由90天縮短到30天甚至更少。」

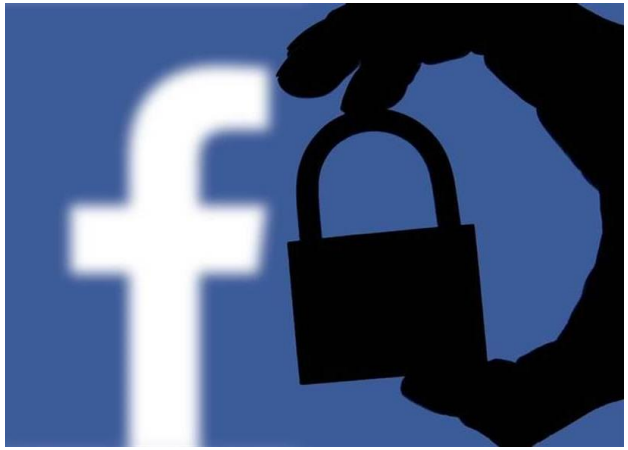
隱私立法

AENEAS

2018年幾起大型數據隱私醜聞在浮出水面，最引人注目的是Facebook的劍橋分析事件安全研究人員認為，2019年在數據隱私方面將會有更多的立法和監管措施。

負責威脅研究的專家表示：「安全與隱私在國會形成了特別的關係，極左激進派與自由主義保守派結成了搭檔。」議員們可能會效仿歐盟的做法，從GDPR的許多方面入手學習。

也就是說，他們的律師和遊說者，早就預料到這一天的到來，
因此，應該由矽谷（而不是華盛頓）來制訂隱私規則。



Thank You

AENEAS