tech FromTheNet

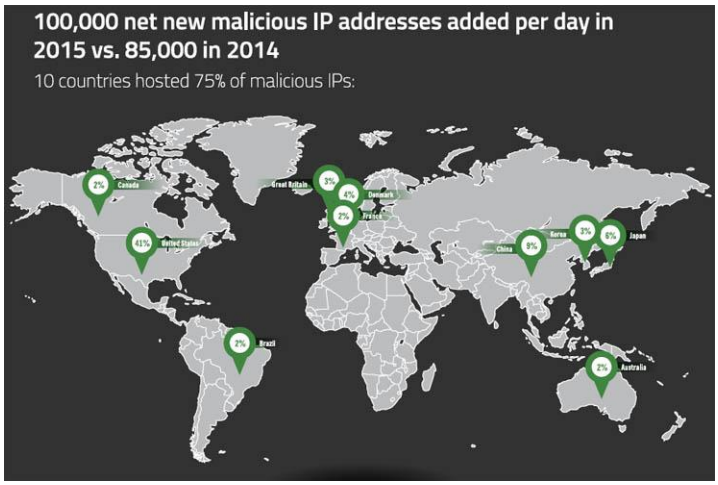
# Webroot Next Generation Threats, le considerazioni di Achab

14 Giugno 2016

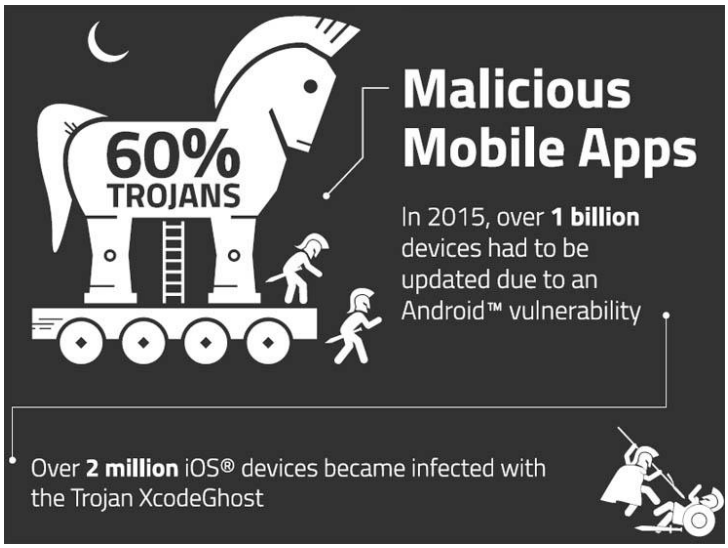
**Achab** analizza il report "Next Generation Threats Exposed" di Webroot, sottolineando l'incidenza dei malware per gli endpoint, gli IP e i siti Web malevoli. **I dati raccolti da Webroot durante tutto il 2015 mostrano inequivocabilmente che oggi gli attacchi sono ormai divenuti globali e fortemente dinamici. Gli esperti Webroot hanno analizzato oltre 27 miliardi di URL, più di 600 milioni di domini, più di 4 miliardi di Indirizzi IP, 9 miliardi di file, 20 milioni di App mobile e 10 milioni di sensori connessi.**

Gli attacchi informatici oggi rappresentano ormai una realtà che non riguarda più solo enti governativi e multinazionali ma interessa anche PMI, liberi professionisti e utenti finali. Essere informati e conoscere le minacce, per scegliere le migliori soluzioni per difendersi dai cyber criminali, è il primo passo per prevenire situazioni di rischio.

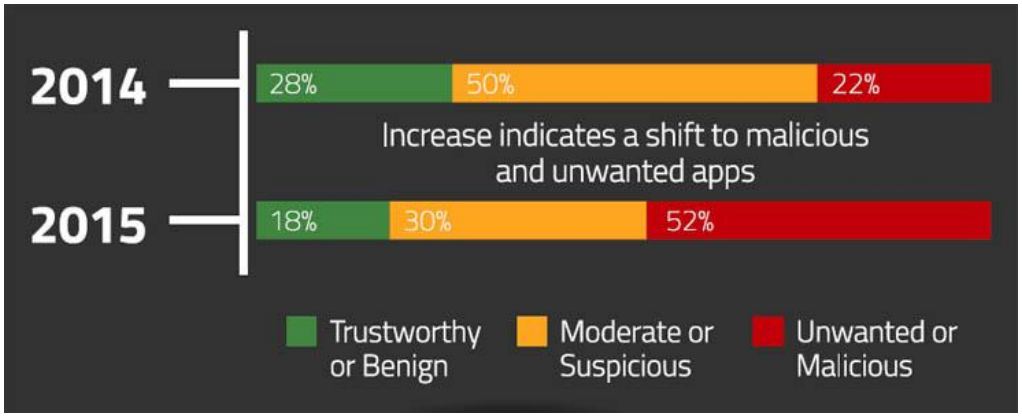
**Malware e applicazioni PUA (Potentially Unwanted Application) sono diventatati polimorfici: oltre il 97% delle istanze di malware rilevate nel 2015 è comparsa su un solo dispositivo.** Ciò significa che il malware di oggi è personalizzato e specifico per ognuno di noi. Altri numeri portano a questa conclusione: i "ceppi" delle applicazioni PUA sono passati da 30.000 nel 2014 a 260 nel 2015. Il "ceppo" di virus è passato da 700 a circa 100. Parallelamente la diffusione dei virus è cresciuta e per spiegare questo fenomeno la chiave di lettura è il polimorfismo, ossia meno "fonti" di virus unici ma con molte più varianti rispetto a prima. Il fatto che i virus cambino in continuazione richiede anche un cambio di azioni nel contrastare i virus. Non sono più sufficienti antivirus che scaricano "le firme" aggiornate perché, se i virus continuano a cambiare velocemente, gli aggiornamento degli antivirus non riescono a reggere questo ritmo: occorre un software di protezione che lavori a più livelli e faccia ricorso a più tecnologie per l'individuazione delle minacce, possibilmente in tempo reale.




Una delle tecniche che si possono usare per fermare il malware è quella di censire i siti che diffondono il malware. **Da anni Webroot continua a tenere aggiornata una lista di indirizzi IP ad alto rischio, lista che oggi conta all'incirca 12 milioni di indirizzi IP. Degli indirizzi che vengono aggiunti ogni giorno alla lista, il 40% risulta non essere mai stato in contatto con attività "malevole", il che dimostra come sia pervasiva la diffusione dei sistemi portatori di virus.**
Gli IP presenti in lista si trovano in tutte le regioni del mondo, anche se le nazioni con il maggior numero di IP presenti in lista (Stati Uniti e Cina) sono largamente davanti a tutti gli altri stati. La maggior parte degli indirizzi IP della lista ha in qualche modo a che fare con lo spam; questi indirizzi inoltre hanno una vita molto breve e sono quindi praticamente impossibili da intercettare utilizzando le "tradizionali" blacklist statiche. Possono essere invece bloccati con sistemi che usano liste dinamiche aggiornate in tempo reale. **Nel corso del 2015 Webroot ha analizzato e classificato milioni di URL e in particolare per il phishing emergono dei numeri interessanti. La probabilità per un utente di incappare in un sito di phishing nel corso del 2015 è del 50% (contro il 30% del 2014), il che testimonia l'efficacia di questo tipo di attacchi.** Le aziende più colpite dal phishing sono le aziende finanziarie e tecnologiche – di seguito la tabella con le Top 5 aziende maggiormente prese di mira nel 2014. Google in particolare la fa da padrone: nel solo 2015 ci sono stati 83.000 siti che si spacciavano per Google cercando di recuperare le credenziali degli utenti. La "classifica" dei Paesi che ospita siti di phishing evidenzia al primo posto gli Stati Uniti e a seguire Regno Unito e Germania.




**Webroot ha analizzato inoltre lo scenario mobile, in questo contesto sono state prese in considerazione oltre 10 milioni di App Android nel solo 2015**. Queste App sono state classificate secondo i parametri “buona”, “dannosa”, “a rischio moderato”, “sospetta”, “indesiderata”. Il 52% di tutte le nuove App sono state categorizzate come indesiderate o dannose, e solo il 18% come buone. E non finisce qui: la maggior parte delle App risultano essere veicolo di virus Trojan (60%) o OUA (28%). Nemmeno gli utenti di iOS non possono considerarsi immuni dagli attacchi: la versione Trojan dell’ambiente di sviluppo Xcode, per esempio, ha infettato 2 milioni di utenti iOS.




Con la crescente diffusione di virus e malware polimorfi appare evidente che le aziende, ma anche i privati, devono fare affidamento su sistemi di sicurezza real-time, per esempio con endpoint di nuova generazione che impediscano agli utenti di entrare in contatto con cybercriminali. I sistemi di intelligenza real-time e basati su cloud permettono di impostare policy proattive per salvaguardare le reti, gli utenti e le informazioni dal dilagante fenomeno del malware.

**Cosa possono fare le aziende e i singoli utenti?**

• *Contrastare le minacce con un approccio innovativo per la rilevazione degli attacchi basati su tecniche fortemente avanzate.*

• *Adottare un approccio alla sicurezza in tempo reale, ad alta precisione e intelligente per*

*contrastare le minacce e per proteggersi dalle attività dei criminali informatici*
*• Impostare politiche proattive per proteggere automaticamente le reti, gli endpoint e gli utenti come parte di una strategia profonda di difesa.*
*• Essere più vigili che mai rispetto ai siti web che si visitano, agli URL che si seguono e alle applicazioni mobile che si utilizzano.*

***Claudio Panerai, CTO Achab***
*Dallo studio emerge che molti attacchi vengono creati, eseguiti e conclusi nel giro di qualche ora e in alcuni casi anche nel giro di pochi minuti. Minuti che bastano per raccogliere credenziali, informazioni personali, crittografare i dati, recuperare informazioni "finanziarie" per accedere a sistemi di internet banking. Contrastare questo tipo di attacchi richiede un approccio innovativo perché è necessario mettere a punto un sistema intelligente a prova di hacker.*