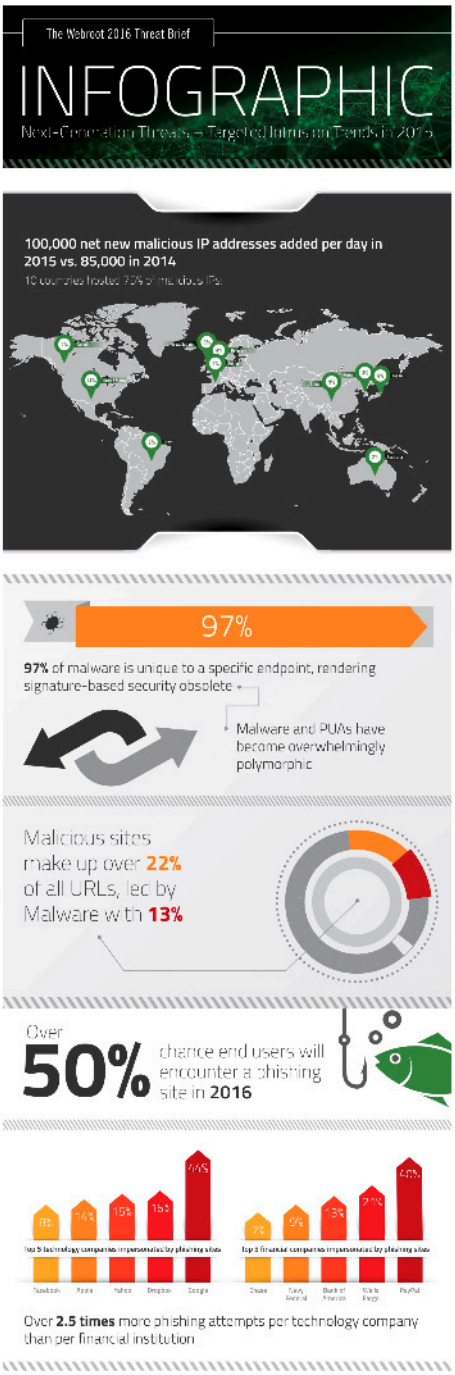
TechWeek europe

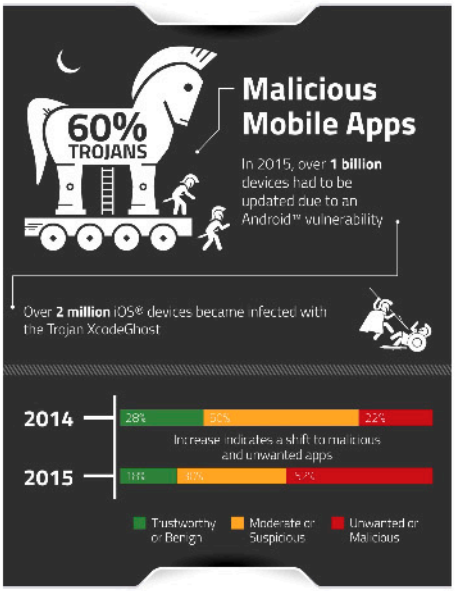
Malware, l'attacco lampo è strategia vincente

Attacchi lampo, mirati, su singoli endpoint, ben ingegnerizzati e di natura polimorfica, questo l'identikit del malware 2.0 che non risparmia le app e richiede un approccio difensivo proattivo. L'infografica Webroot, l'analisi del report e una strategia difensiva



Webroot ha pubblicato il suo report definitivo relativo alle minacce del 2015 – ***Next Generation Threats Exposed*** è il suo nome – sulla base del quale è possibile evidenziare i trend più importanti relativi alle minacce web, in ogni loro forma, che hanno messo a rischio dati, infrastrutture e business a livello mondiale. Subito alcuni macro elementi: è cresciuto il numero di indirizzi IP malevoli, anno su anno (100mila nel 2015, mentre erano 85mila l'anno prima), oltre il 20 percento dei siti web contiene codice malevole, e oltre il 10 percento di essi vero e proprio malware, le vulnerabilità di Android hanno costretto all'aggiornamento oltre un miliardo di dispositivi nell'anno scorso, e circa 2 milioni di smartphone e tablet iOS sono stati infettati dal Trojan XcodeGhost. Quasi la totalità dei malware è scritta nello specifico per ogni endpoint, mentre sono i nomi delle aziende più conosciute quelli utilizzati con maggiore frequenza per i tentativi di phishing che rappresenta ancora il sistema migliore per infettare gli ambienti. Sulla scorta di queste cifre analizzate in dettaglio, spiegano gli esperti di sicurezza di **Achab** (distributore delle soluzioni **Webroot**), è possibile ricostruire uno scenario per cui tanti attacchi vengono eseguiti e conclusi nel giro di poche ore, in qualche caso di pochi minuti, mentre acquista grande importanza per gli hacker tutta la fase di preparazione prima di sferrare l'attacco, la fase di ingegnerizzazione e quella di scrittura del codice. Nei pochi minuti dell'attacco vengono raccolti dati, informazioni personali e finanziarie, e vengono crittografati i record che saranno utilizzati e rivenduti.

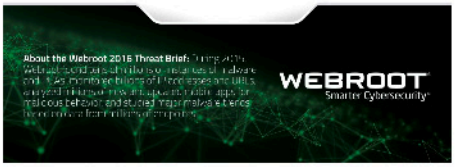
Approccio vincente è sempre ottimizzare il più possibile la parte più impegnativa del lavoro, quella di preparazione, e quindi poi essere in grado di attaccare anche più volte variando il minimo necessario per non essere riconosciuti. Da qui il riscontro sulla pericolosità di malware



2015 clearly shows that today's threats are global and highly dynamic, **but what can companies and individuals do?**

- Countering threats requires an innovative approach to attack detection based heavily on advanced techniques.
- Organizations need to bolster their security posture with real-time, highly accurate threat intelligence to protect themselves from cybercriminal activity.
- Admins should set proactive policies to automatically protect networks, endpoints, and users as part of a defense-in-depth strategy.
- Individuals need to be more vigilant than ever about the websites they visit, the URLs they follow, and the applications and mobile apps that they use.

Read the full Webroot 2016 Threat Brief at:
www.webroot.com/Webroot-2016-Threat-Brief.pdf



Infografica Webroot 2015/2016

e applicazioni polimorfici, da qui quel 97 percento di istanze malware comparse su un solo dispositivo, quindi malware del tutto su misura per la singola vittima, ma con un ceppo comune il cui numero invece va riducendosi (quello delle PUA da 30mila nel 2014 a 260 nel 2015 e quello dei virus da 700 a circa 100). L'approccio degli antivirus sulla base di "firme" aggiornate è antico, e gli antivirus non riescono a supportare la rapida integrazione di tutte le firme.

Webroot ha analizzato nel corso dell'anno oltre 27 miliardi di URL, più di 600 milioni di domini, 9 miliardi di file, 20 milioni di app per dispositivi mobile, e anche i sensori in ambito Iot. Si tratta di una superficie di attacco che deve oramai portare ad atteggiamenti responsabili anche le piccole e medie imprese e i singoli utenti finali, la prima arma di difesa è sempre la consapevolezza. Inoltre una delle tecniche che più paga nel fermare il malware è censire le fonti da cui provengono (indirizzi IP), pur consapevoli che solo il 40 percento di essi si rivelerà non essere mai stato a contatto con codice malevolo, che essi avranno vita breve e si potranno bloccare solo sfruttando tecnologiche di listing dinamiche.
Il phishing resta l'arma più utilizzata, nel 2015 oltre 83mila siti hanno tentato di spacciarsi per Google, nella lista anche Microsoft, Apple, tutti nomi conosciuti agli utenti che avranno almeno un servizio di questi tre vendor utilizzato, nomi quindi che permettono di sferrare l'attacco su un bacino di utenti illimitato.

In ambito mobile si conferma come la fiducia nelle app sia infinitamente maggiore rispetto alla loro effettiva reputazione. Secondo Webroot il 52 percento di tutte le nuove app sono da categorizzare come indesiderate o dannose, e solo il 18 percento sarebbe valido da tutti i punti di vista. La maggior parte delle app sono risultate veicolo di virus Trojan (circa il 60 percento) o OUA (nel 28 percento dei casi). **Con la versione Trojan dell'ambiente di sviluppo Xcode, per esempio, che ha infettato 2 milioni di utenti iOS**. Il mantra per Webroot è prima di tutto, oltre la consapevolezza, è fare affidamento su una valida soluzione di protezione dell'endpoint in realtime, intelligenti, basati su cloud con la possibilità di impostare policy proattive e la fuga di informazioni dal device verso indirizzi malevoli.