Vulnerabilità

Massimo Carnevali

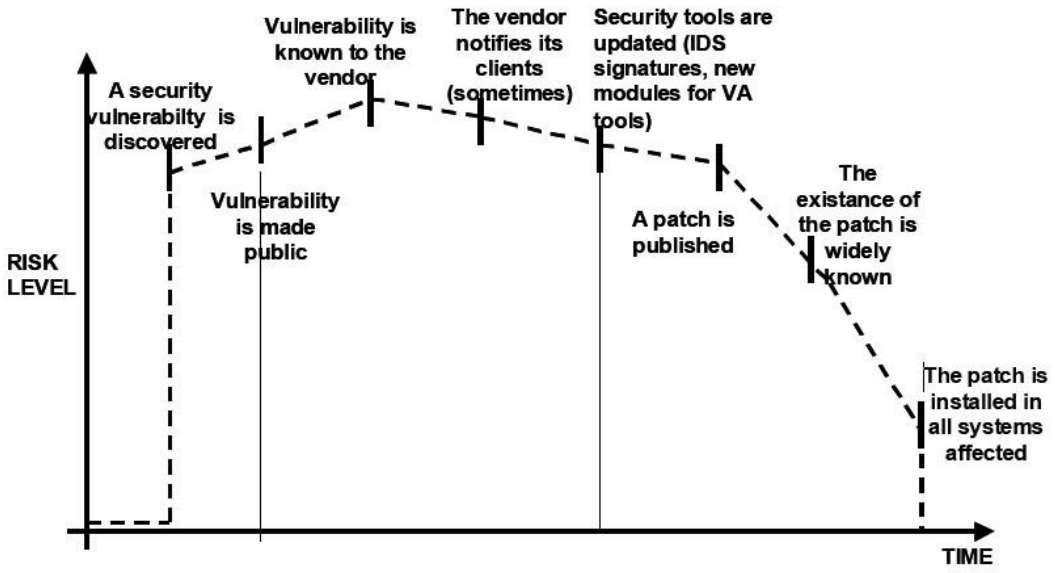
Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

Vulnerabilità

- Il concetto di vulnerabilità e il suo ciclo di vita

..

Vulnerabilità



Full disclosure come filosofia (dibattito)
https://en.wikipedia.org/wiki/Full_disclosure_(computer_security)

Parziale (ne parlo prima con il vendor) o totale (tutto subito). Pro e contro.
Patching è un costo esterno senza nessun valore per il produttore
(tipo inquinamento, mi debbono "costringere" a mettere i filtri per non inquinare).

Fonte: OWASP
https://www.owasp.org/index.php/Testing_Guide_Introduction

Vulnerabilità

Zero Day Vulnerability

Window of exposure = ∞

https://en.wikipedia.org/wiki/Zero-day_(computing)

Una vulnerabilità scoperta ma non resa pubblica (nemmeno al produttore).

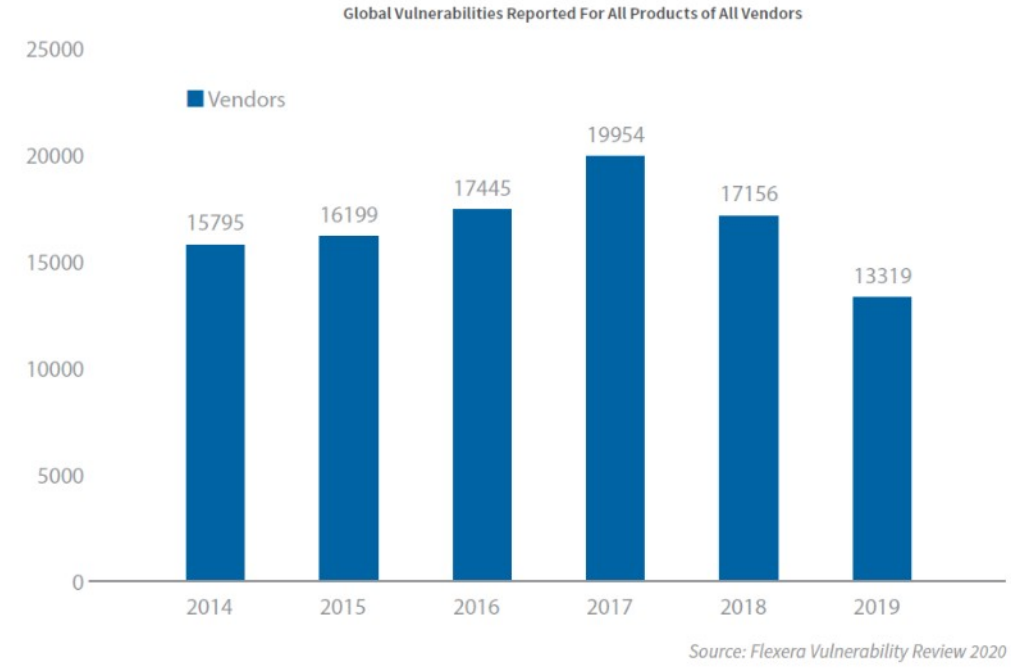
Solitamente rivendute oppure tenute da parte per operazioni redditizie (anche governative).

Window of exposure infinita (o almeno finché qualcuno non se ne accorge).

Business nemmeno più nascosto

https://zerodium.com/

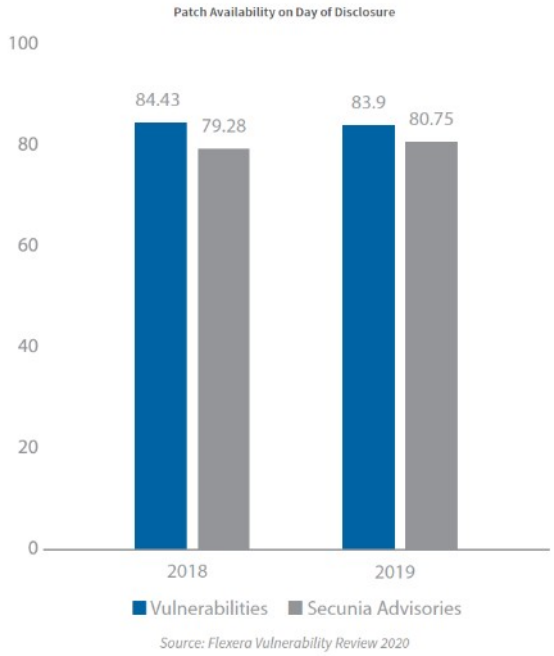
Vulnerabilità



Fonte Flexera Vulnerability review 2020
https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020

Tendenza al miglioramento.

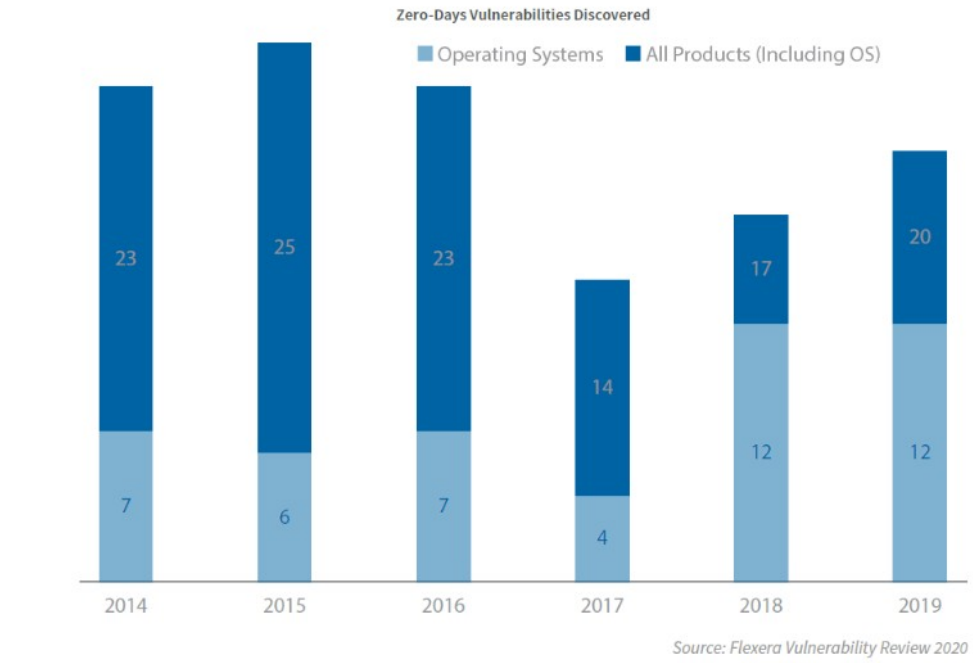
Vulnerabilità



Fonte Flexera Vulnerability review 2020
https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020

Nell’84% dei casi patch disponibile il giorno stesso della segnalazione della vulnerabilità. Il rimanente 16% probabilmente non verrà mai patchato (vendor non esiste più, software fuori manutenzione ecc.)

Vulnerabilità

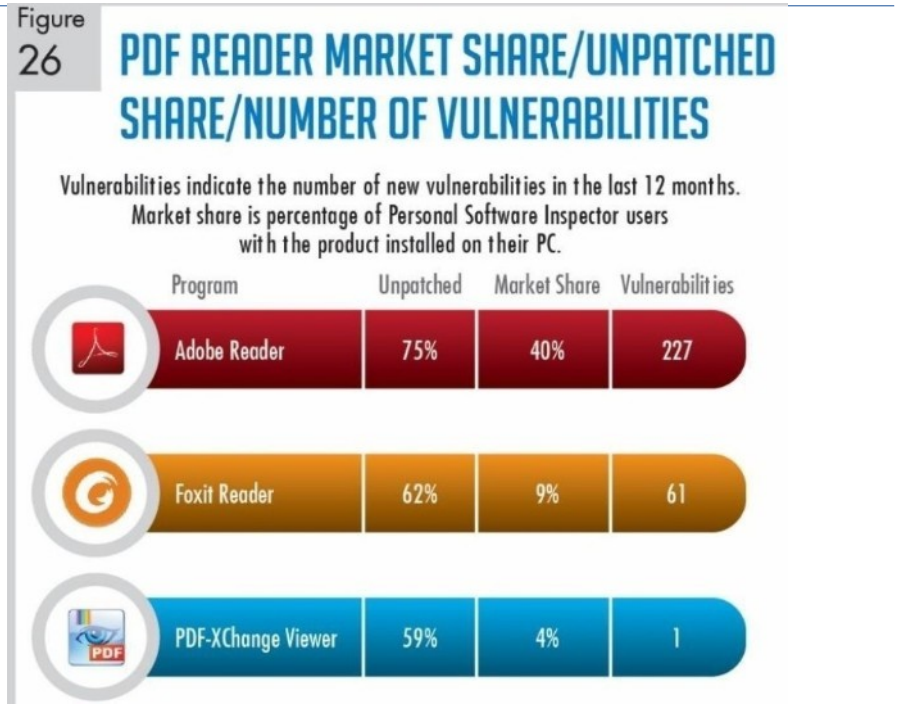


 7

Fonte Flexera Vulnerability review 2020
https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020

Pochi zero day scoperti: perché chi li ha scoperti è bravo a tenerli segreti? (se li uso in un attacco rischio di farmi scoprire e di perdere lo zero day)

Vulnerabilità



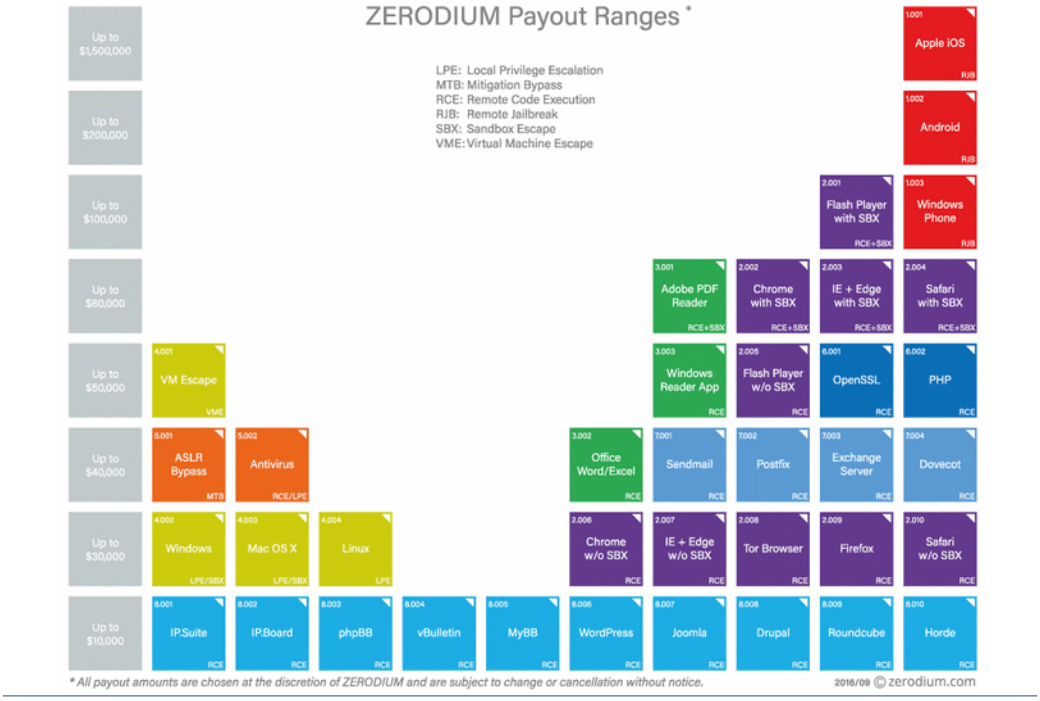
Fonte Flexera Vulnerability review 2017
http://www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/

Quindi Acrobat Reader è:

- Diffuso
- Bucato
- Non patchato

Una manna per un attaccante!

Vulnerabilità



Quanto paga Zerodium per una vulnerabilità zero day.
(vedi anche la parte su “chi sono i cattivi”)

Patch management

http://en.wikipedia.org/wiki/Patch_(computing)
E' un sottoproblema del configuration management di particolare impatto sulle metodologie per la sicurezza dei sistemi.
To patch or not to patch?
Questa domanda ha una risposta risolvendo il problema seguente: il rischio di applicare al sistema la patch è superiore al rischio della vulnerabilità che la patch corregge?
E' un calcolo difficile e comunque deve essere effettuato all'interno di una metodologia chiara e ben pianificata.

Una corretta metodologia di patch management
può essere espressa in varie fasi
1. Baseline definition
2. Test Environments
3. Backout Plans
4. Patch collection and evaluation
5. Consolidation
6. Deployment
7. Reporting