



Frodi online e Cybercrime

Cosa li accomuna e come mitigarli

Giovanni Napoli - RSA Pre-Sales Manager

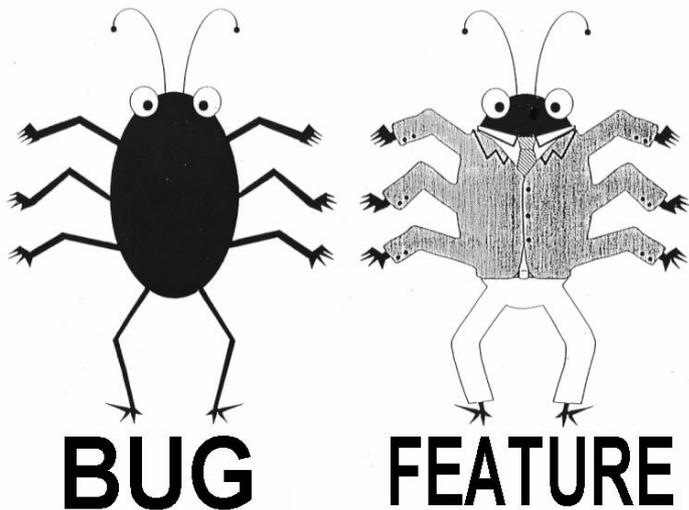
La cruda realtà del software engineering

- Non e' possibile dimostrare la correttezza formale di un software
- Semplici contesti informatici a volte mal si prestano ad essere modellati e validati matematicamente
- Dobbiamo imparare a convivere con vulnerabilita' che hanno un elevato rapporto costi/benefici

Rischio = Minaccia x Vulnerabilità x Impatto

La cruda realtà del software engineering

Scarsa progettazione software diventa feature

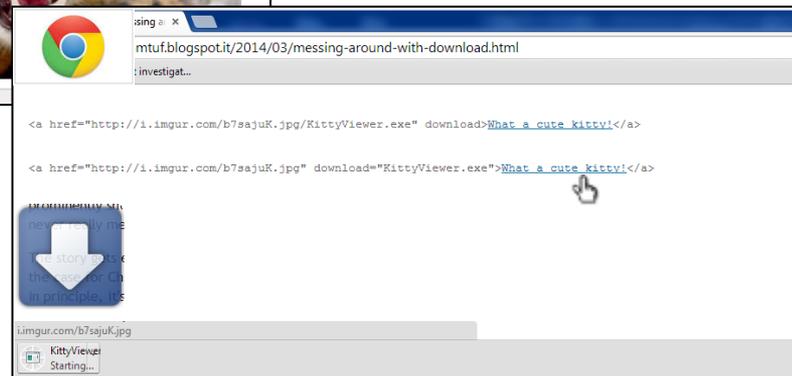
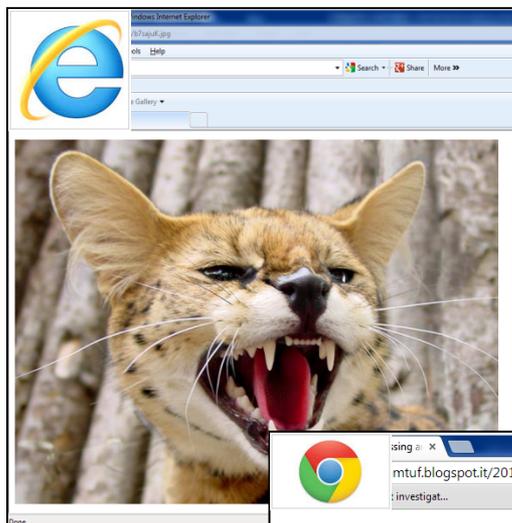
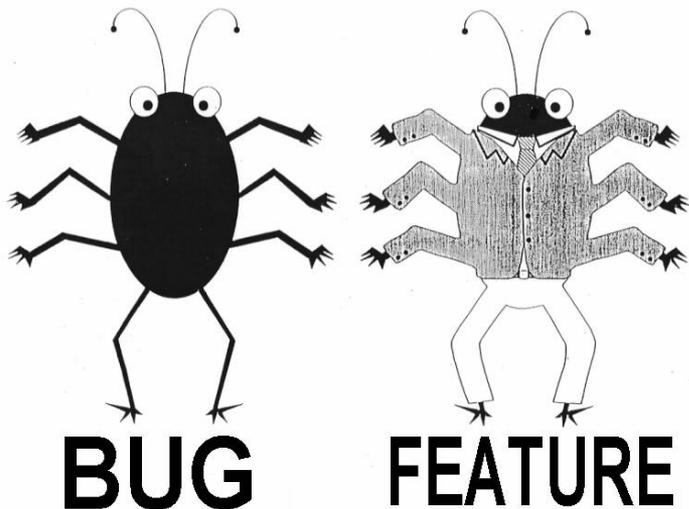


```
http://i.imgur.com/b7sajuK.jpg/KittyViewer.exe
```

```
http://i.imgur.com/b7sajuK.jpg
```

La cruda realtà del software engineering

Scarsa progettazione software
diventa feature

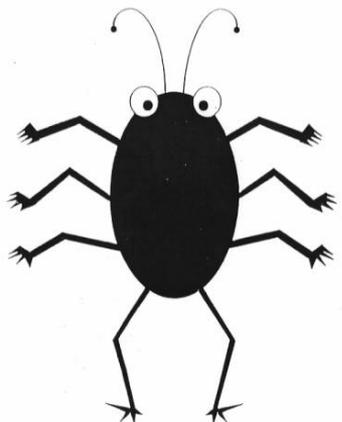


`What a cute kitty!`
`What a cute kitty!`

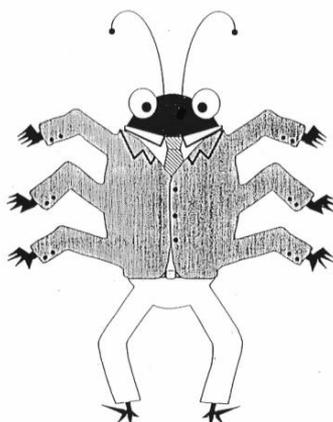
Provatele ad esempio con Internet Explorer e Chrome...

La cruda realtà del software engineering

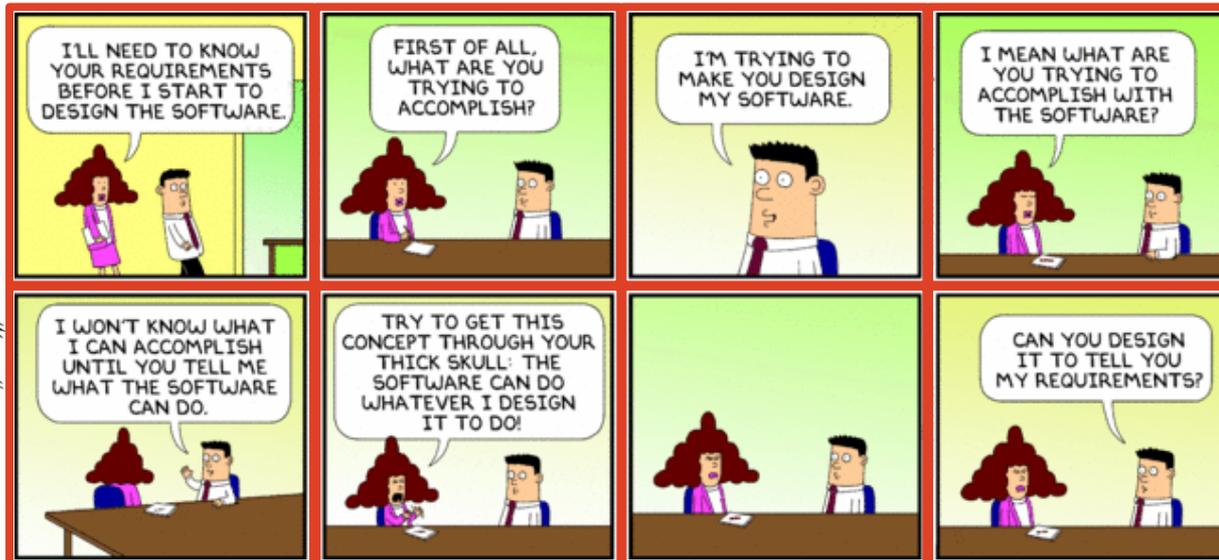
Scarsa progettazione software diventa feature



BUG



FEATURE



Carenza di requisiti che guidano software a supporto di processi aziendali

Un grave esempio: Heartbleed

Che cos'è?

- Un bug in OpenSSL
 - OpenSSL dalla 1.0.1 fino alla 1.0.1f sono vulnerabili
 - OpenSSL 1.0.1g NON e' vulnerabile
- Un banale errore di programmazione

```
/* Read type and payload length first */  
hbtype = *p++;  
n2s(p, payload);  
p1 = p;
```

Bug

```
hbtype = *p++;  
n2s(p, payload);  
if (1 + 2 + payload + 16 > s->s3->rrec.length)  
    return 0; /* silently discard per RFC 6520 sec. 4 */  
p1 = p;
```

Fix

OR `-DOPENSSL_NO_HEARTBEATS` → At recompile time

- Il bug e' probabilmente presente fin da marzo 2012

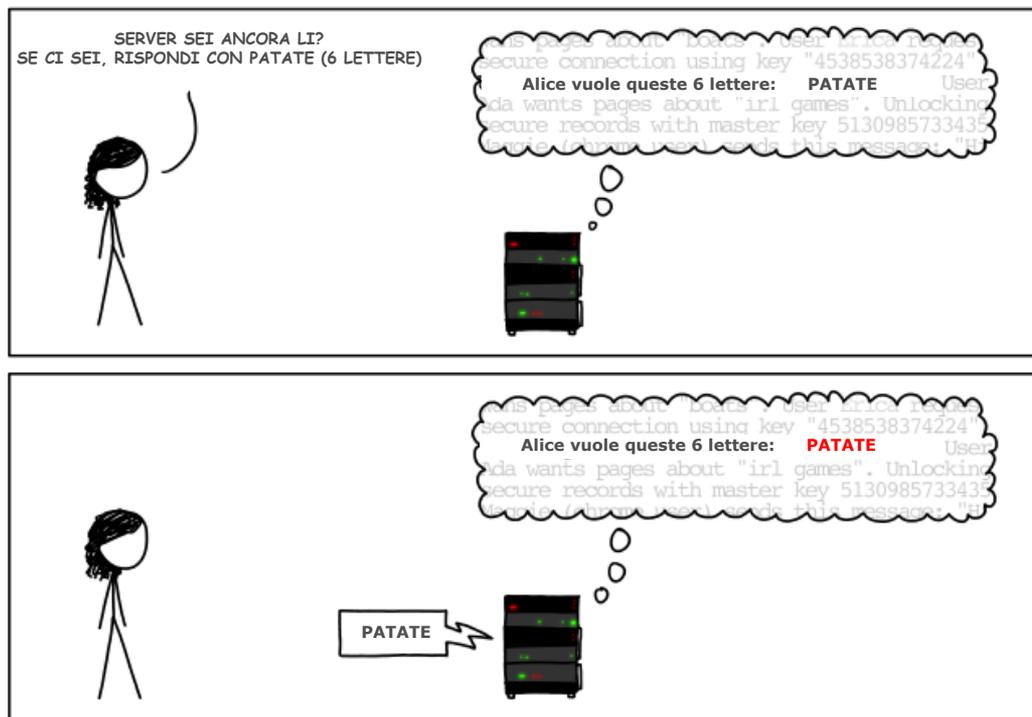
Un grave esempio: Heartbleed

Quali sono gli impatti?

- Un server affetto dalla vulnerabilità è soggetto a perdite di dati sensibili tra i quali:
 - Password
 - User Login
 - SSL Private Key
- Un certificato SSL Server è pubblico. Se un attacker possiede la chiave privata associata, la sola cosa che manca è un semplice attacco DNS
- Bug exploit che non lascia traccia...

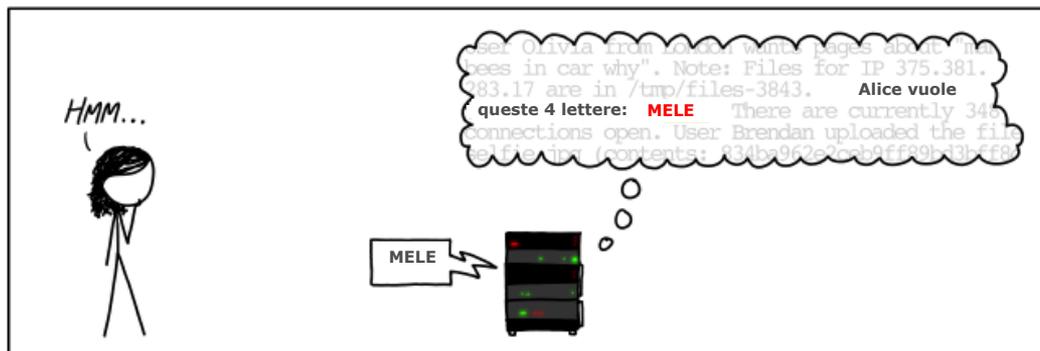
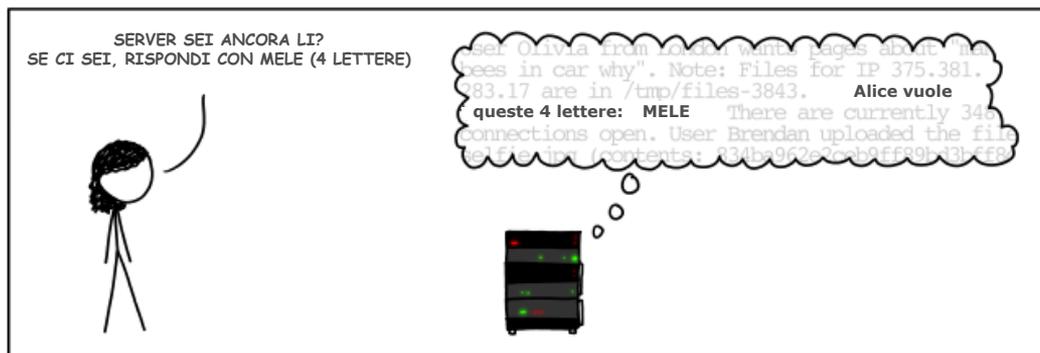
Un grave esempio: Heartbleed

Come funziona?



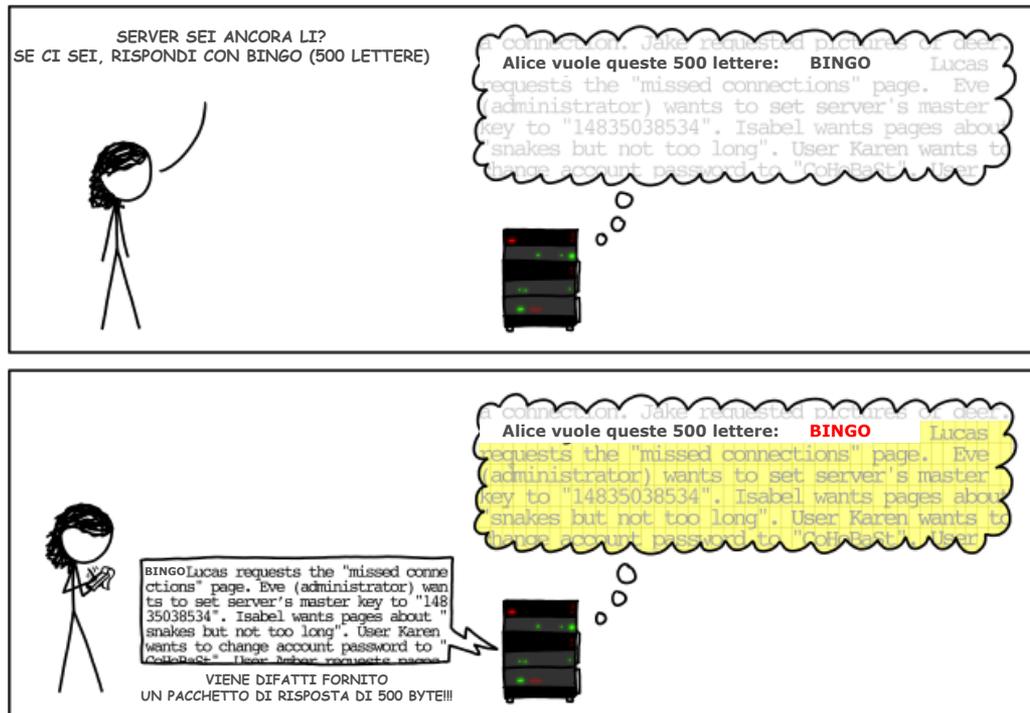
Un grave esempio: Heartbleed

Come funziona?



Un grave esempio: Heartbleed

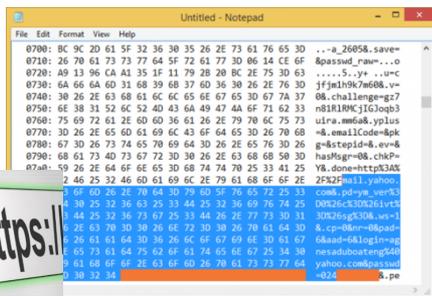
Come funziona?



Heartbleed in ambito frodi e cybercrime

Ricordiamoci sempre le motivazioni degli attacker...

Ambito frodi



```
0700: BC 9C 2D 01 5F 32 36 30 35 26 2E 73 61 76 65 3D ...a_26058.save=
0710: 26 70 61 73 73 77 64 5F 72 61 77 3D 06 14 CE 6F 8passud_ran...o
0720: A9 13 96 CA A1 35 1F 11 79 28 20 BC 2E 75 30 63 ....S..y...uc
0730: 6A 66 64 60 31 68 39 68 37 60 36 26 76 30 63 ffe1197d6d8.vv
0740: 30 26 2E 63 68 61 6C 6E 65 6E 67 65 30 67 7A 37 08.challenge-gz7
0750: 6E 38 31 52 6C 52 40 43 6A 49 47 4A 6F 71 62 33 n81R1RMJCjGloqb3
0760: 75 69 72 61 2E 60 60 36 61 26 2E 79 70 6C 75 3 uira.mm68.yplus
0770: 30 26 2E 65 60 61 69 6C 43 6F 64 65 30 26 70 68 -8_emailCode-8pk
0780: 67 30 26 73 74 65 70 69 64 30 26 2E 65 76 30 26 g-8stepid-8_ev-8
0790: 68 61 73 40 73 67 72 30 26 2E 63 68 68 50 3D hasM8r-08.chkP=
07a0: 59 26 2E 64 6F 6E 65 30 68 74 70 25 33 41 25 Y8_done=http3KAX
07b0: 2 46 25 32 46 50 61 69 6C 2E 79 61 68 65 6F 2E 252219011sym000
07c0: 6F 60 26 2E 70 64 30 79 60 5F 76 65 72 25 33 com_pd-ye_ver93
07d0: 30 25 32 36 63 25 33 44 25 32 36 69 76 74 25 D0R26ck3Dk261vt3
07e0: 44 25 32 36 73 67 25 33 48 26 2E 77 73 30 11 30R26gk1D8_wst-1
07f0: 25 63 70 30 38 26 72 30 39 70 61 64 30 8_czp-8b0m-08pam
0800: 26 61 63 64 30 26 6C 6F 67 69 6E 30 61 67 6kaud-6klog1-mag
0810: 65 73 61 64 75 62 6F 61 74 65 6E 67 25 34 30 mesadubosteng5d8
0820: 61 68 6F 6E 63 6F 6D 26 70 61 73 73 72 64 yahoo.compassua
0830: 19 32 34 -0b4 .rpe
```



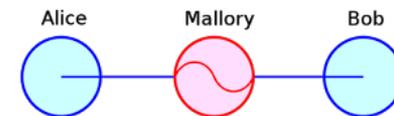
- Phishing
- Collezionare indirizzi email, login, password



Catastrophic...
...Up to 11

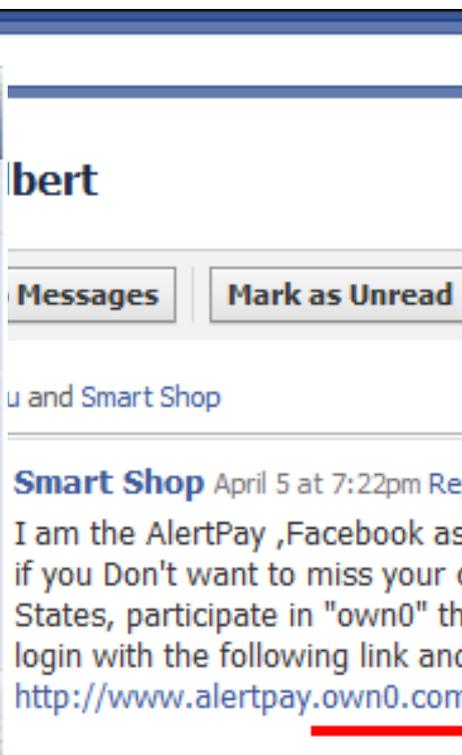


Ambito cybercrime

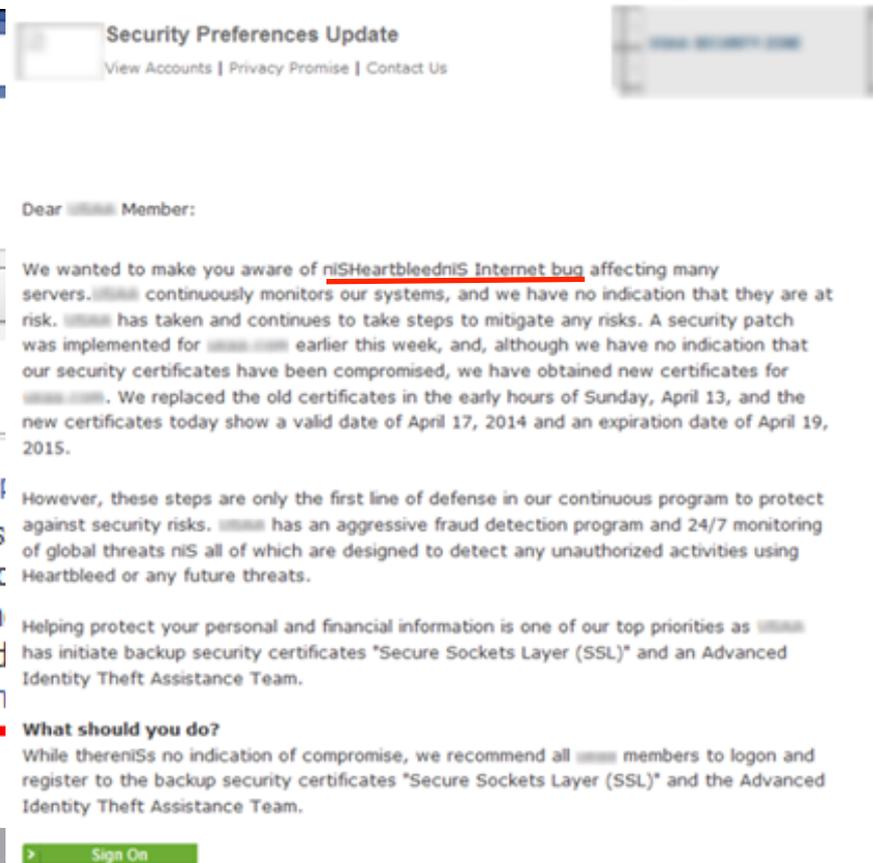


- Intercettare comunicazioni private
- Impersonare utenti e servizi
- Rubare dati sensibili senza la necessità di avere privilegi particolari

Phishing e Social Engineering trovano ovunque



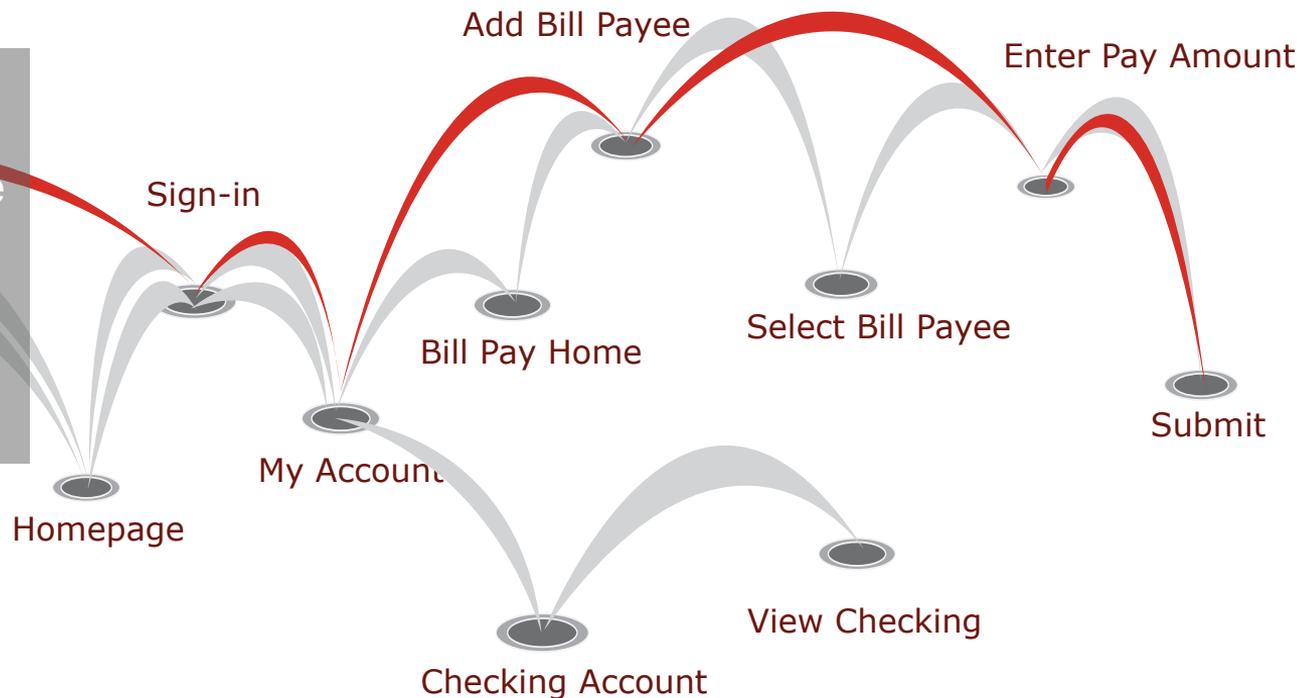
GOOD LUCK



Analisi Comportamentale è Essenziale

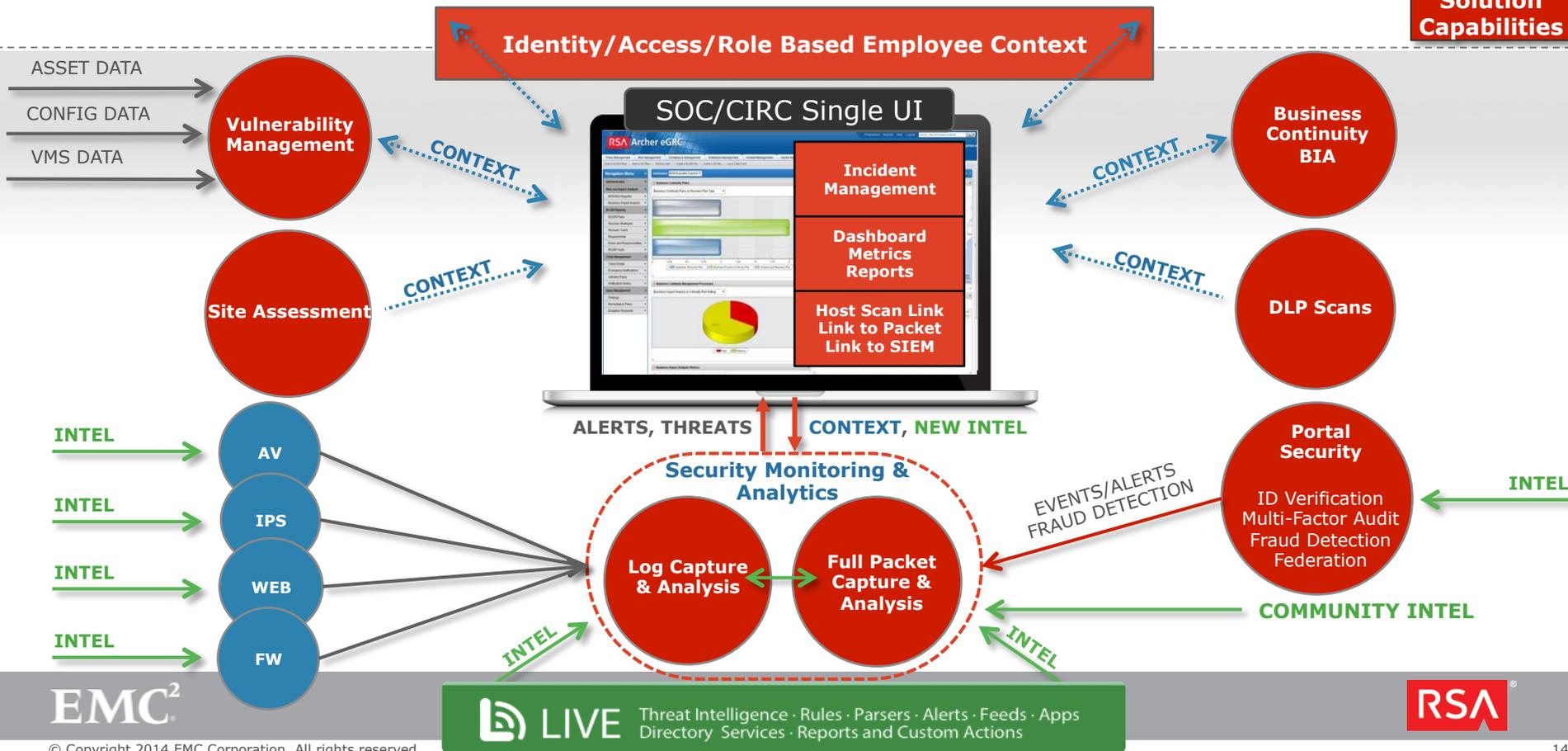
I criminali si comportano diversamente da utenti legittimi

- Velocità
- Sequenza delle pagine
- Origine
- Contesto
- Comportamento

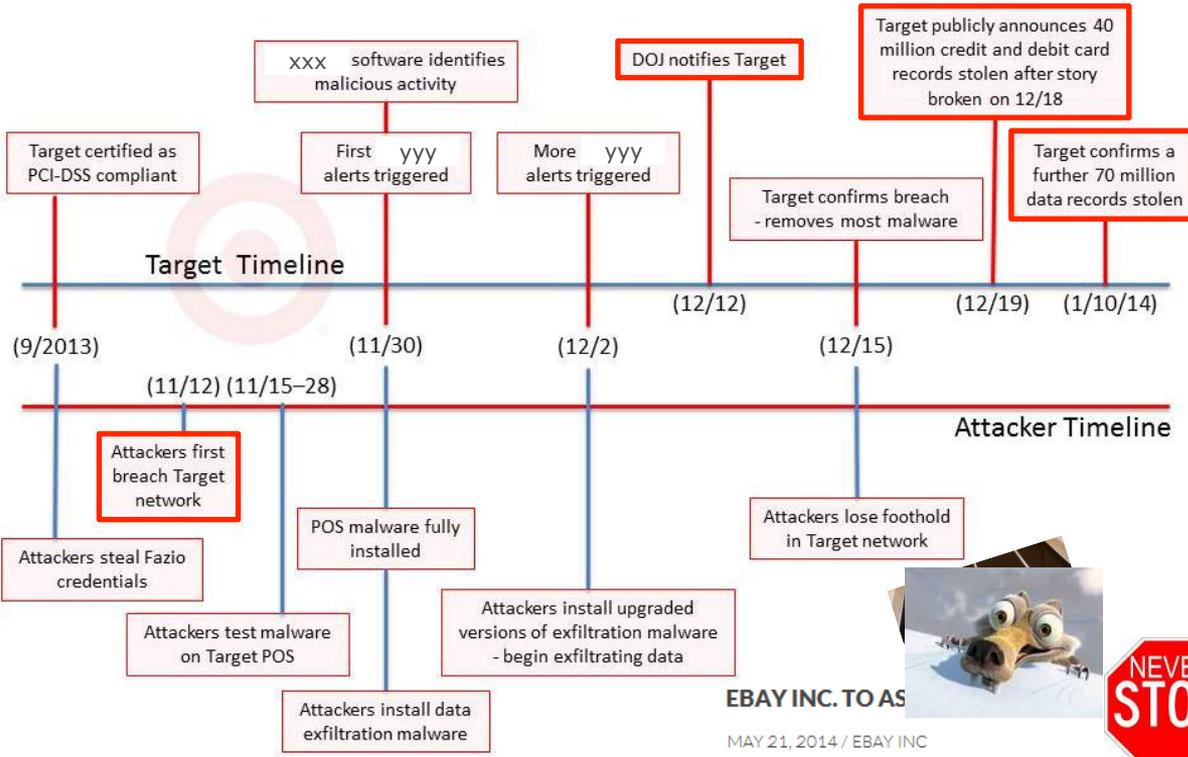


Come mitigare attività di cybercrime

RSA
Solution
Capabilities



Target Data Breach: Approccio RSA



- L'attacco ha sfruttato la debolezza di un Partner
- Target si è perso gli alert di difesa perimetrale
- L'attacker ha sfruttato la debolezza dei controlli per espandere il suo perimetro d'azione
- Target si è perso anche gli eventi legati all'asportazione dei dati aziendali

Avrebbe forse potuto disporre di un efficace framework di Governance Risk e Compliance per mantenere tutti ed i soli controlli di sicurezza necessari? Avrebbe forse potuto disporre di piu' efficaci strumenti di investigazione, di capacità di integrazione di informazioni di intelligence e di maggiore competenza del proprio personale o dei propri consulenti...?



Azienda - Integrare le informazioni di intelligence all'interno della nostra infrastruttura ed organizzazione IT



EMC²®

@RSAItalia