Frodi online e Cybercrime

Cosa li accomuna e come mitigarli

Giovanni Napoli - RSA Pre-Sales Manager

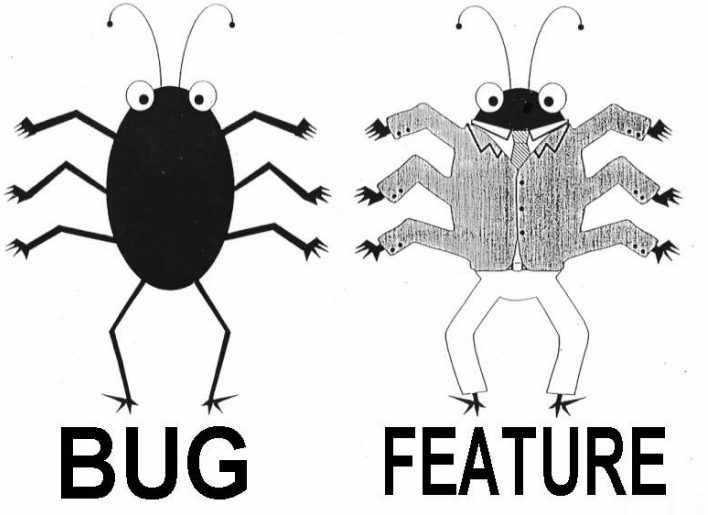
La cruda realtà del software engineering

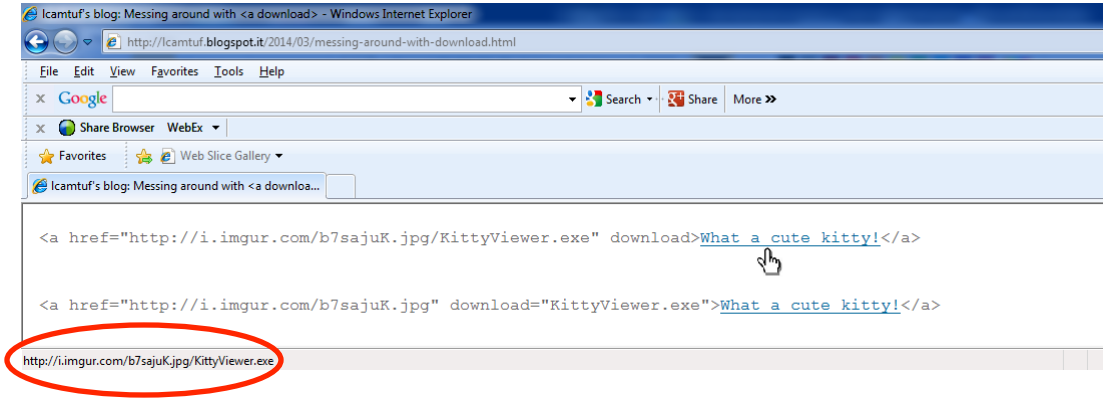
- Non e' possibile dimostrare la correttezza formale di un software
- Semplici contesti informatici a volte mal si prestano ad essere modellati e validati matematicamente
- Dobbiamo imparare a convivere con vulnerabilita' che hanno un elevato rapporto costi/benefici

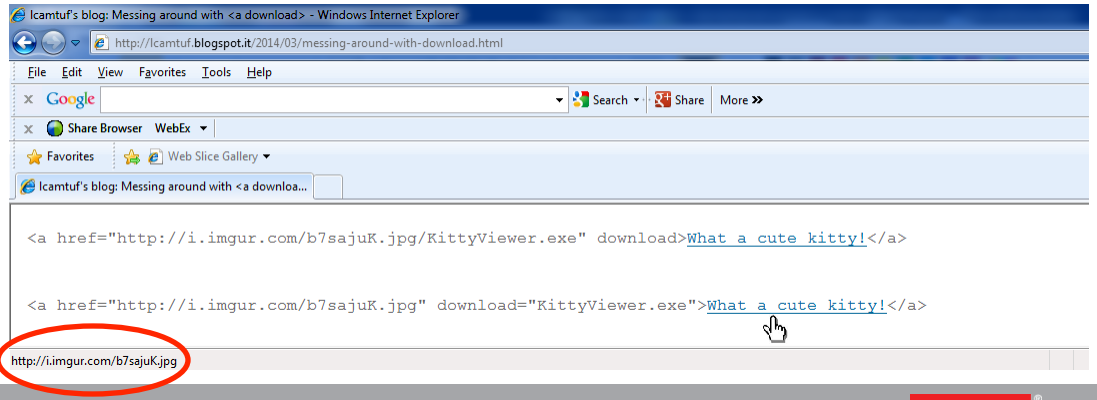
Rischio = Minaccia x Vulnerabilità x Impatto

La cruda realtà del software engineering

Scarsa progettazione software diventa feature

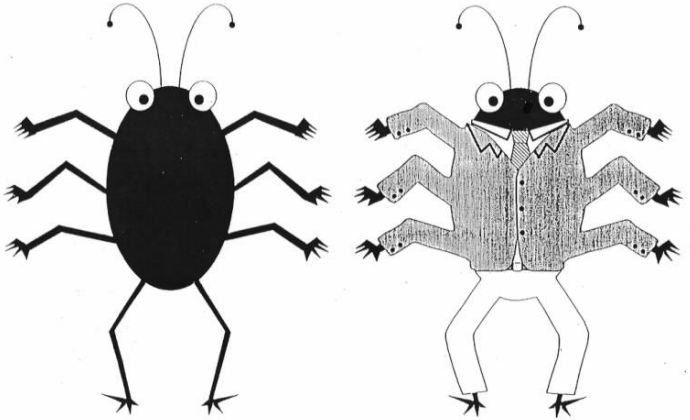


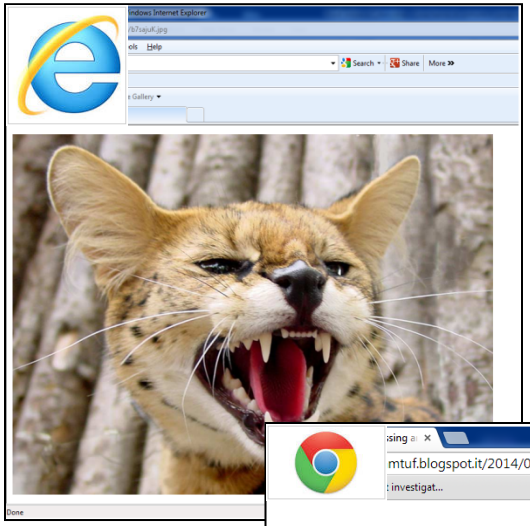


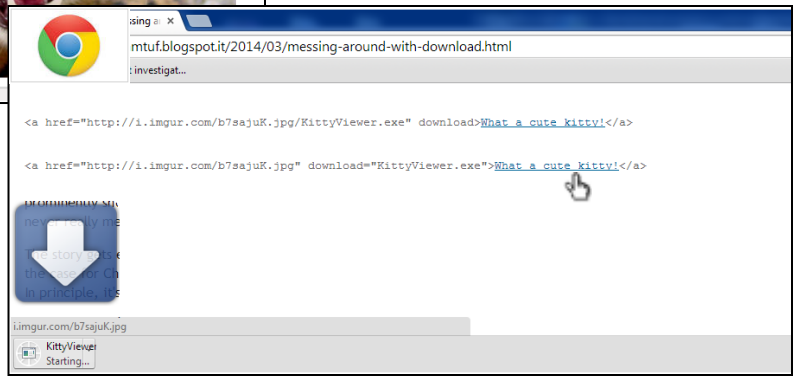


La cruda realtà del software engineering

Scarsa progettazione software diventa feature





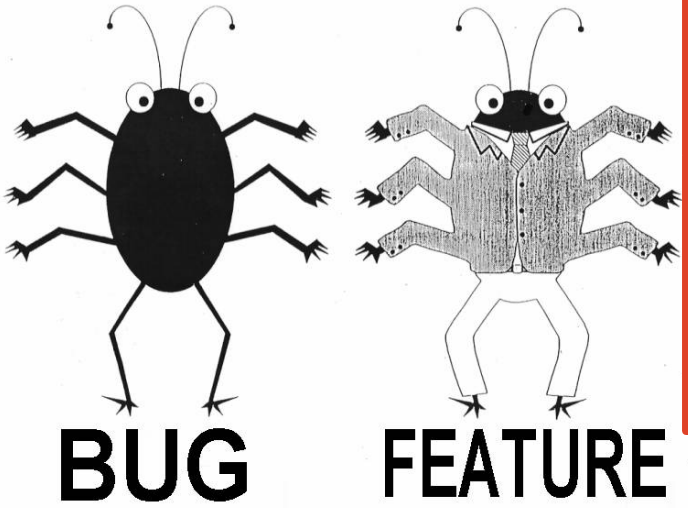


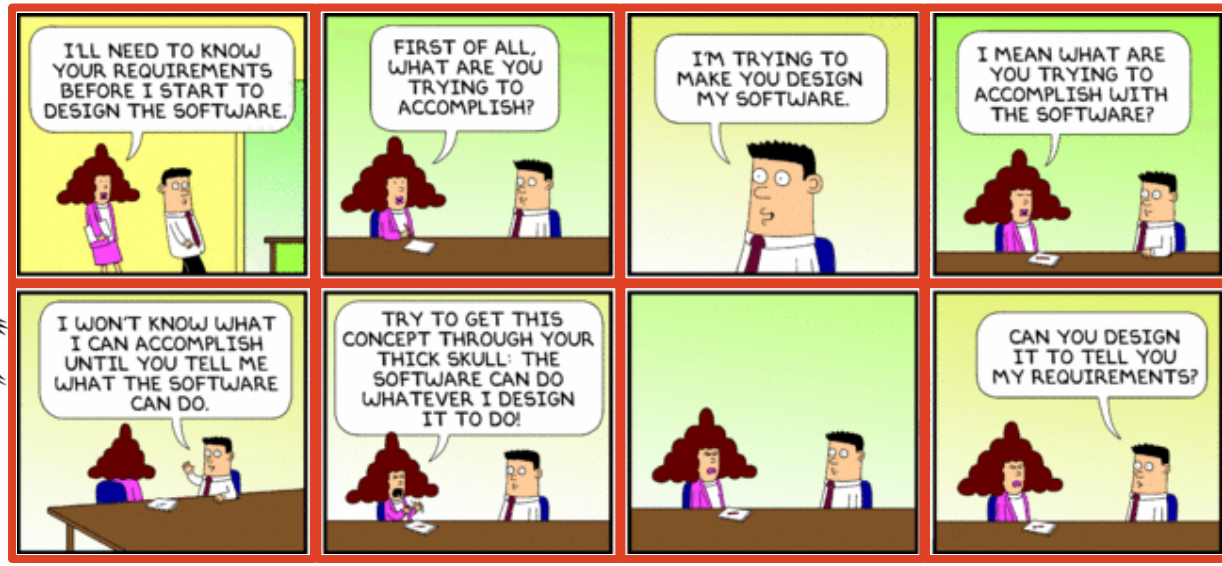

```
<a href="http://i.imgur.com/b7sajuK.jpg/KittyViewer.exe" download>What a cute kitty!</a>
<a href="http://i.imgur.com/b7sajuK.jpg" download="KittyViewer.exe">What a cute kitty!</a>
```

Provatelo ad esempio con Internet Explorer e Chrome…

La cruda realtà del software engineering

Scarsa progettazione software diventa feature





Carenza di requisiti che guidano software a supporto di processi aziendali

Un grave esempio: Heartbleed

Che cos'é?

- 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

Bug

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

Fix

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

OR `-DOPENSSL_NO_HEARTBEATS` → At recompile time

- Il bug e' probabilmente presente fin da marzo 2012

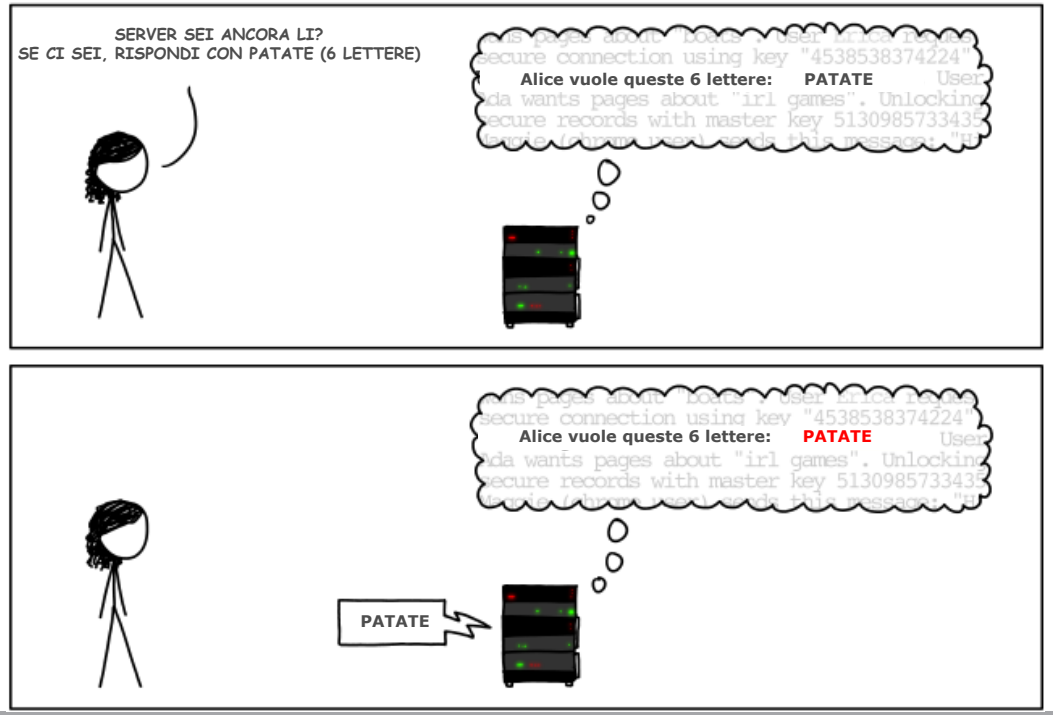
Un grave esempio: Heartbleed

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…

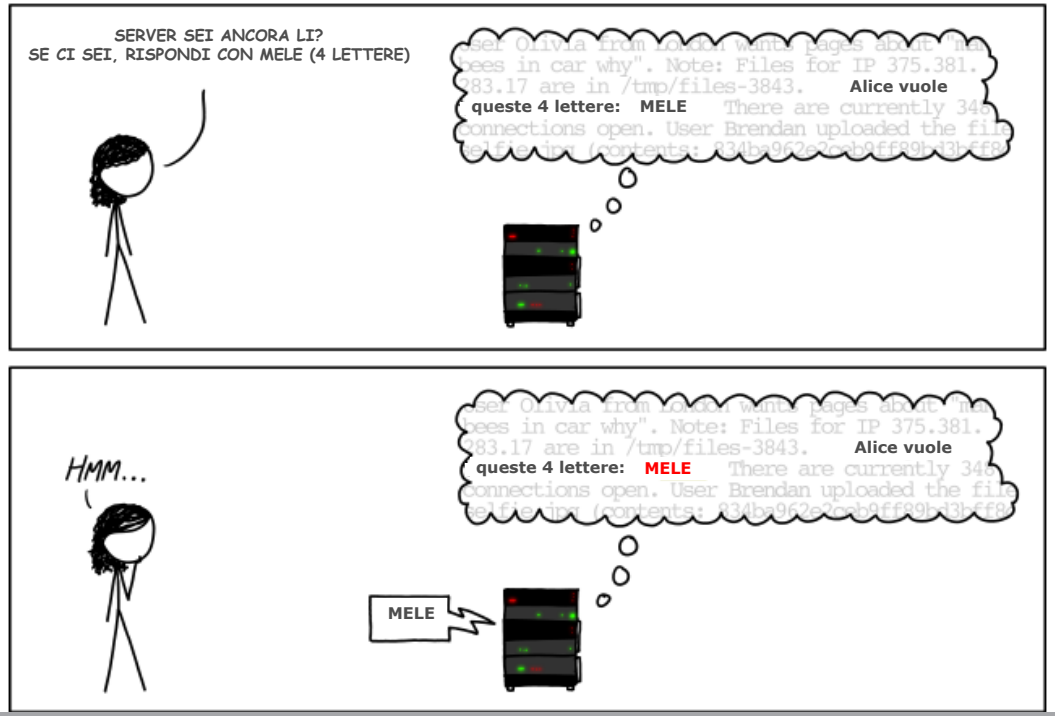
Un grave esempio: Heartbleed

Come funziona?



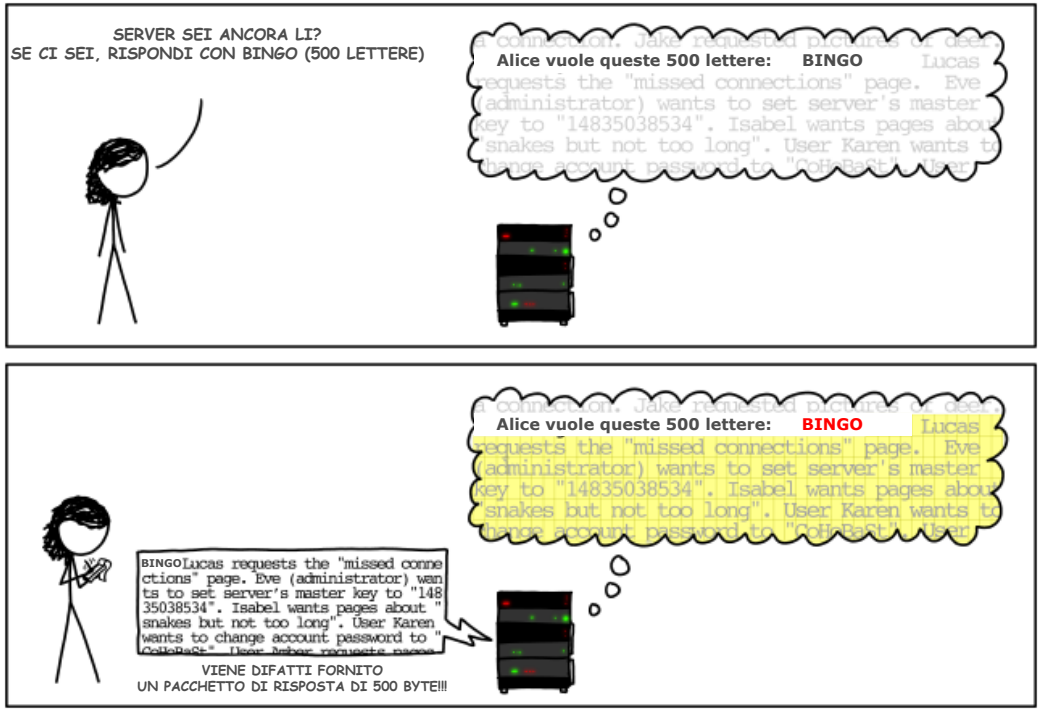
Un grave esempio: Heartbleed

Come funziona?



Un grave esempio: Heartbleed

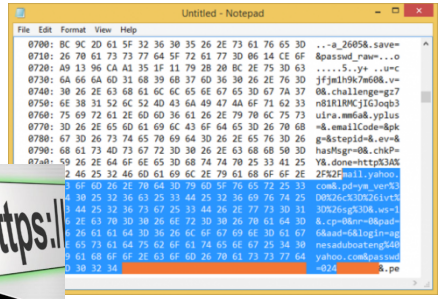
Come funziona?



Heartbleed in ambito frodi e cybercrime

Ricordiamoci sempre le motivazioni degli attacker…

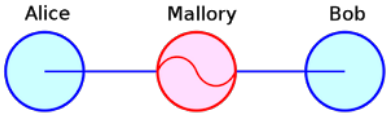
Ambito frodi



- Phishing
- Collezionare indirizzi email, login, password

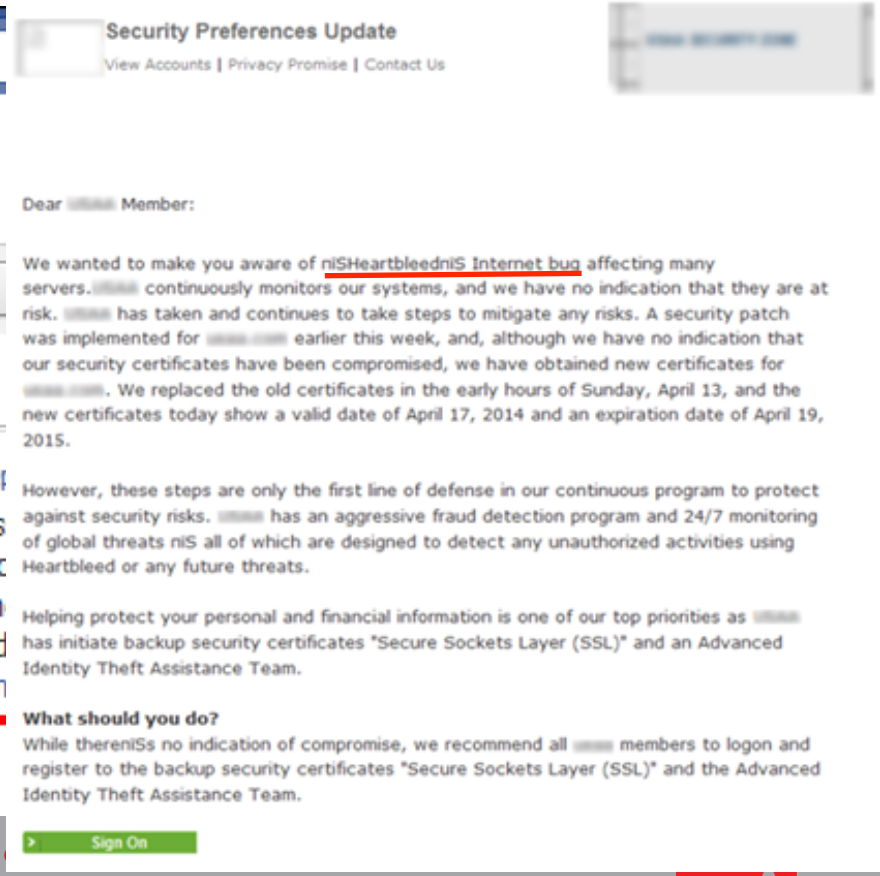
Catastrophic…
…Up to 11

Ambito cybercrime



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

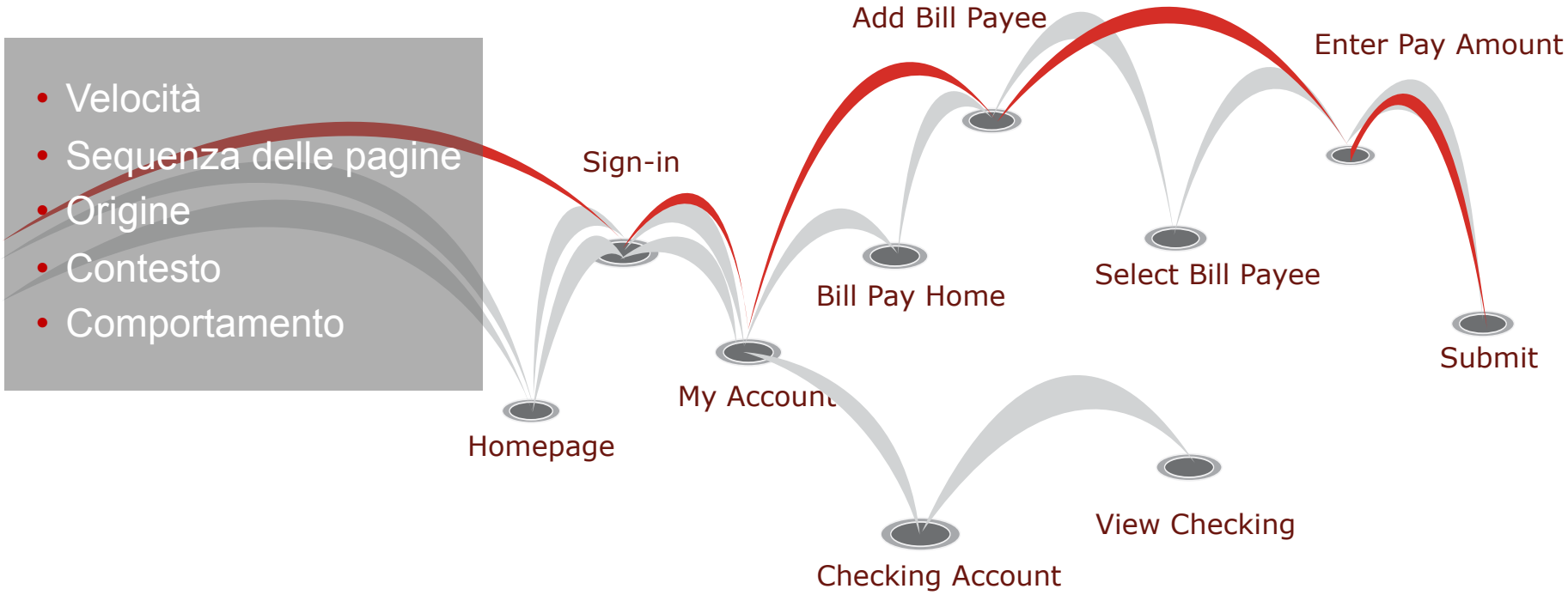
Phishing e Social Eng ti trovano ovunque



Analisi Comportamentale è Essenziale

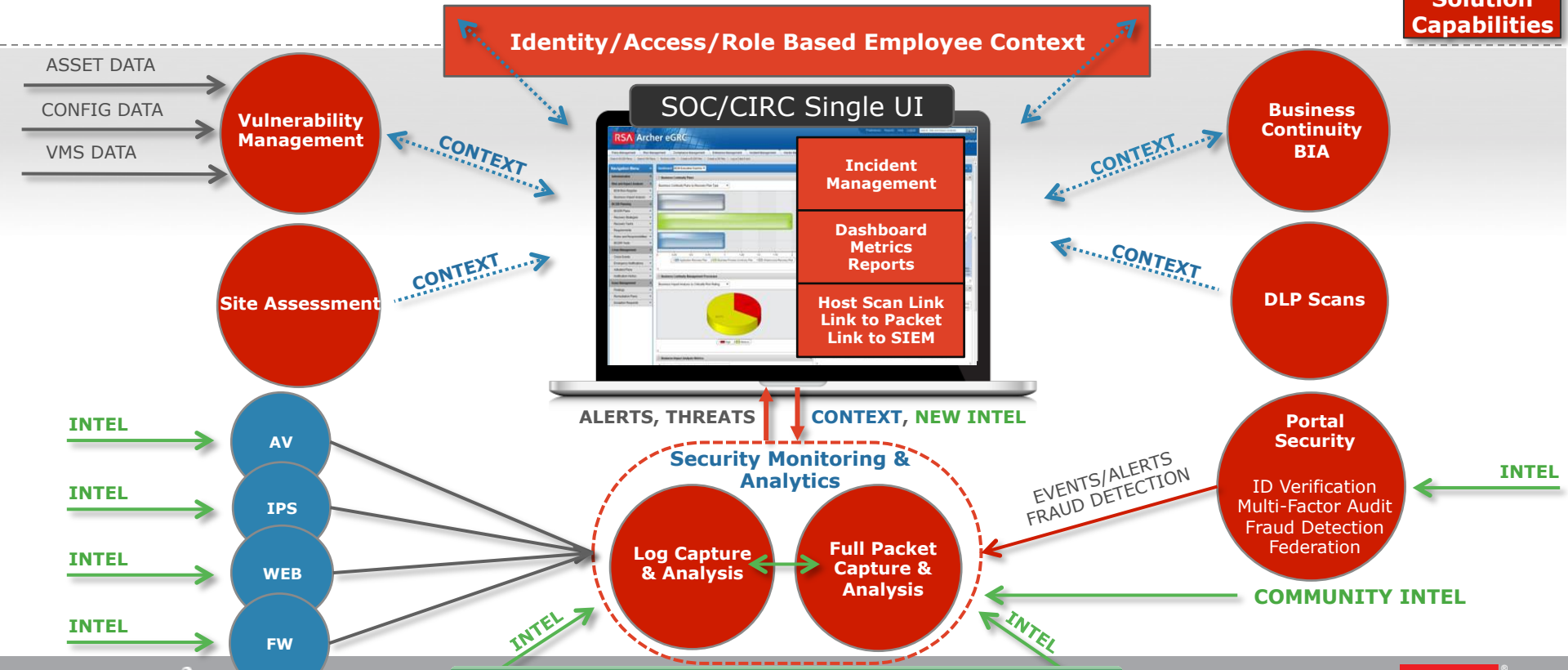
I criminali si comportano diversamente da utenti legittimi

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

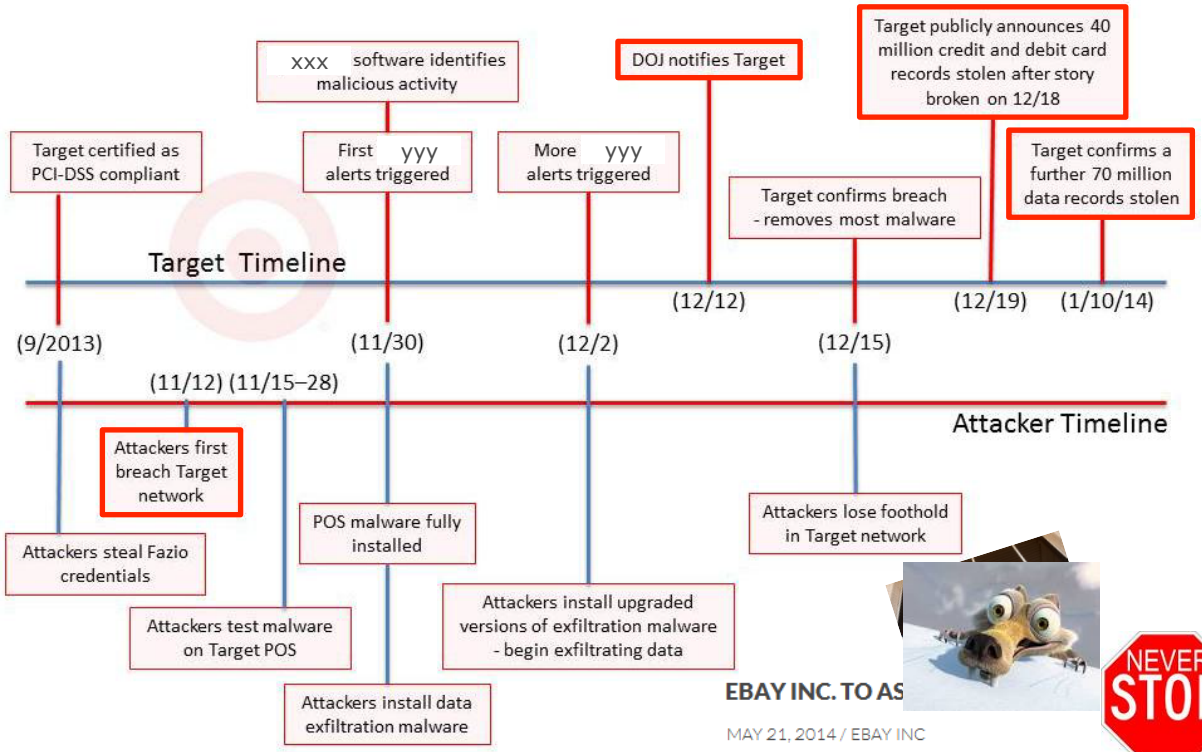


Come mitigare attività di cybercrime

RSA Solution Capabilities



Target Data Breach: Approccio RSA



EBAY INC. TO AS SSWORDS

MAY 21, 2014 / EBAY INC

https://blog.ebay.com/ebay-inc-ask-ebay-users-change-passwords/

- 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 manutenere 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

Intelligence Driven Security

@RSAItalia