



From Web Attacks to Malware

Can Secure Software Development Help Internet Banking Security?

Giorgio Fedon
Owasp Italy – Technical Director

giorgio.fedon@mindedsecurity.com

**OWASP
Day IV**

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

Presentazione

■ Ricerca

- ▶ OWASP Italy - Technical Director
- ▶ OWASP Antimalware project leader
- ▶ Testing Guide Contributor
- ▶ Analisi e scoperta di importanti problematiche di sicurezza

■ Minded Security

- ▶ Chief Operation Officer
- ▶ Leading hundreds of Penetration Testing activities and Code Reviews; many of them for the Bank Industry
- ▶ Blog: <http://blog.mindedsecurity.com>



Costruire e sviluppare senza la giusta qualità



Recenti News

- ▶ 2005 - Una banca Svedese ha avvisato la stampa che i suoi clienti sono stati frodati per 700000 euro attraverso l'uso di uno specifico malware
- ▶ 2007 - "*Silent Banker* Trojan crea attacchi mirati per 400 Banche ed è in grado di effettuare il bypass di modalità di autenticazione a più fattori"
- ▶ 2008 - Un attacco di SQL Injection ad "Heartland Payment Systems" rivela i dati di circa 100 Milioni di carte di credito
- ▶ 2009 - Un attacco di phishing ad una banca Spagnola permette agli attaccanti di impadronirsi di circa 10000 credenziali degli utenti



Le modalità di attacco più ricorrenti

■ Phishing

- ▶ Email inviate agli utenti dall'attaccante con link a siti fasulli

■ Malware Bancario

- ▶ Software in grado di manipolare i contenuti web visionati e inviati dall'utente

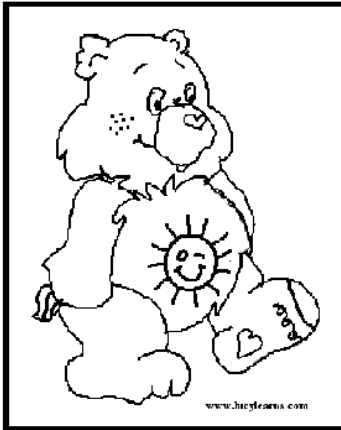
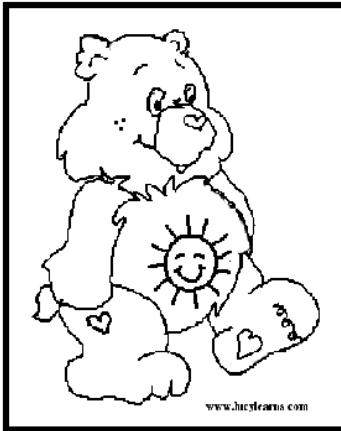
■ SQL Injection

- ▶ Accesso alla base dati direttamente dal portale di internet banking



Veloce confronto fra le precedenti categorie

Spot 5 differences



- Modalità *note al settore da diversi anni*
- Colpiscono *ambiti differenti* (utenti vs infrastruttura)
- Efficacia *alta* con effort relativamente *basso* (attacchi in gran parte automatizzabili)

L'attaccante cerca l'anello debole

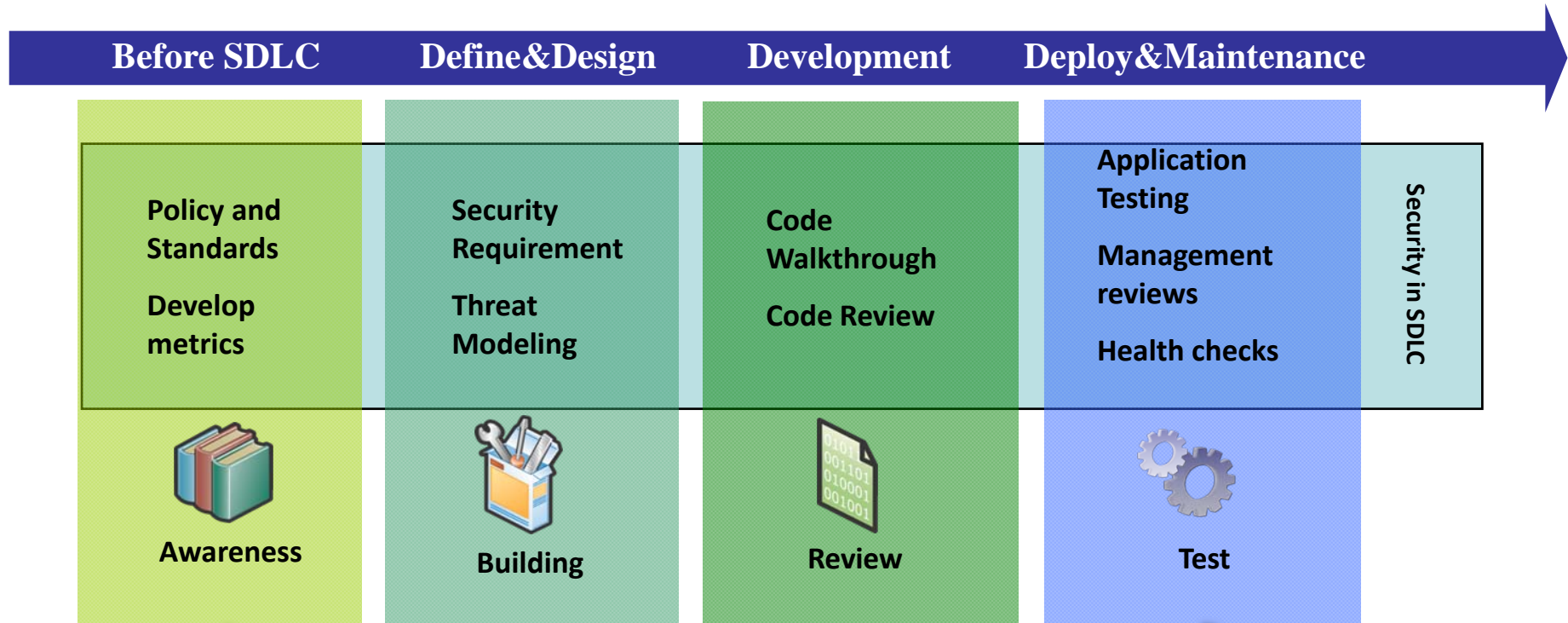
- L'attenzione indirizzata verso solo alcuni aspetti, ne indebolisce altri



- Importante è creare un piano nello sviluppo delle applicazioni per una migliore razionalizzazione delle risorse



Piano di Sicurezza nello Sviluppo



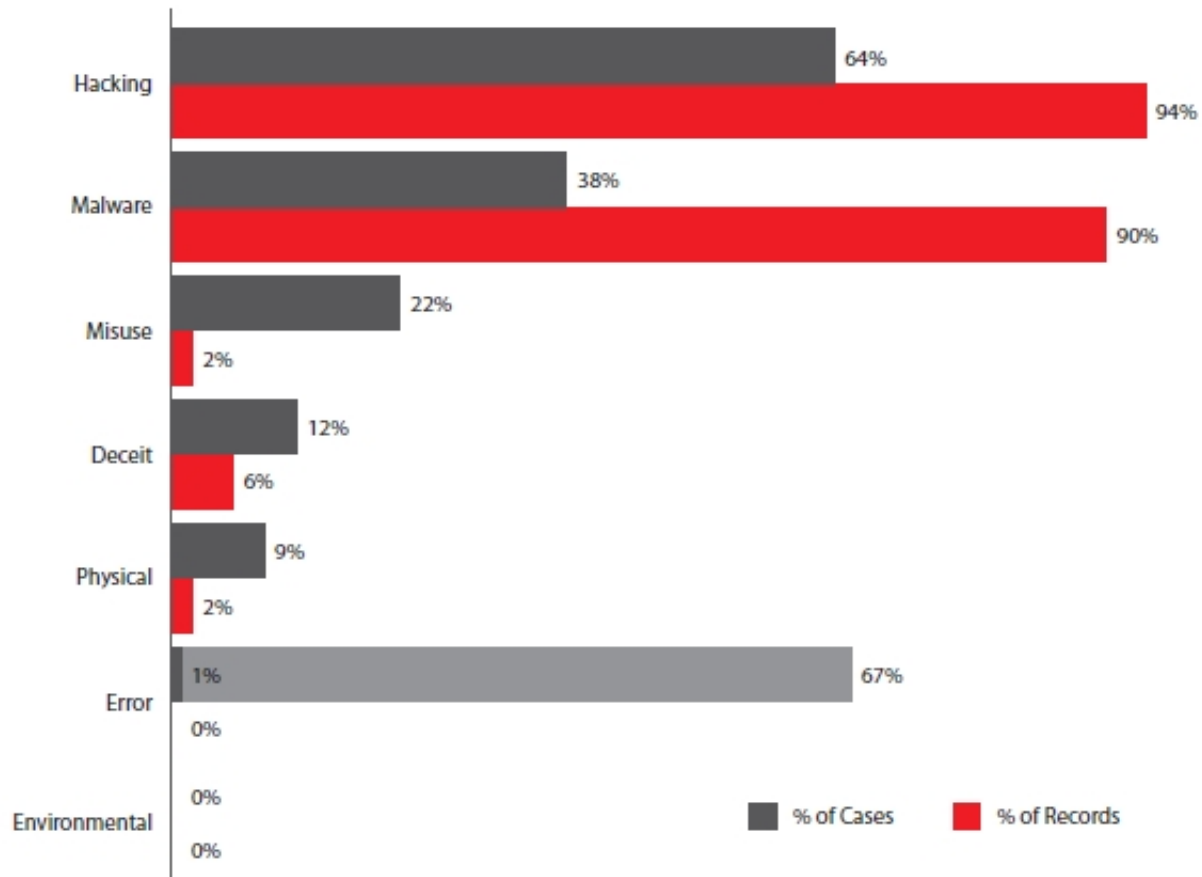
Il ciclo si ripete su base temporale, in vista delle problematiche riscontrate e dei nuovi sviluppi



Banking Attack Process



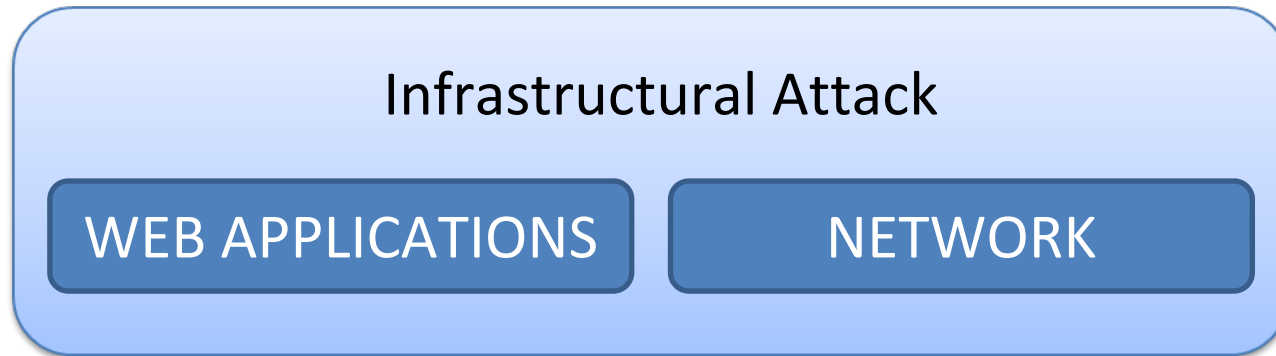
Alcune statistiche



Source: Verizon Data Breach Report 2009



Attacchi all'infrastruttura



1. Tecniche di scansione mediante tool automatizzati per ricercare problematiche infrastrutturali
2. Dalle statistiche le problematiche "Web" di data validation e configurazione rappresentano più del 60% degli attacchi infrastrutturali effettuati con successo
3. Il target si considera raggiunto nel caso in cui l'attaccante trovi importanti vulnerabilità



Toolset "cinese" per attacchi di SQL Injection

The screenshot shows the 'Toolset' application interface. At the top, the URL is set to `http://localhost/sqlinject/news.asp?id=1`. The interface includes tabs for '总体输出', '基本信息', '探测设置', 'HEAD', 'Cookies', and '浏览'. Below these are buttons for '另存为...', '保存', '复制', and a checked option for '同时输出到表格'. The left sidebar contains sections for '远程服务器列表' (listing NTJ-S4\GSQ), '登录用户列表' (listing user 'testDB.admin'), and a 'SQL Server' section with buttons for 'SQL Server', 'Access', 'MySQL', and 'Oracle'. The main area shows a 'where:' field with `1=1` and a 'SQL:' field with `select top 3 id,username,password from TestDB..admin order by id`. The '当前库' is 'TestDB' and the '排序' is 'id'. A table displays the results of the query:

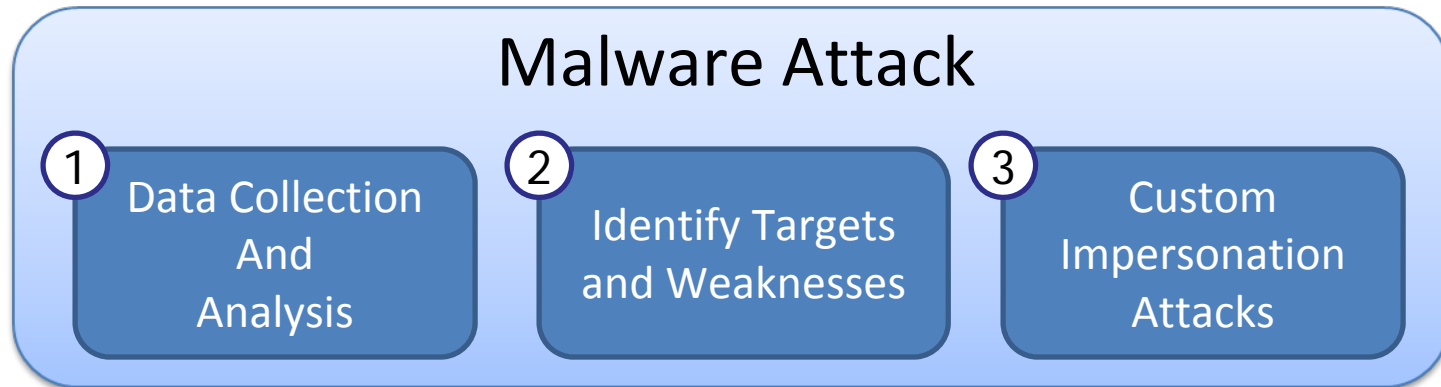
id	username	password
1	testUserzjs	123456
25	test	password
26	ff	aa

Three callout boxes provide additional information:

- L'attaccante specifica l'url del sito dove effettuare la ricerca di SQL Injection** (The attacker specifies the URL of the site where to perform the SQL Injection search).
- Il tool ha funzioni integrate per estrarre i dati** (The tool has integrated functions to extract data).
- Costo del tool \$50 dollari!** (Cost of the tool \$50 dollars!).



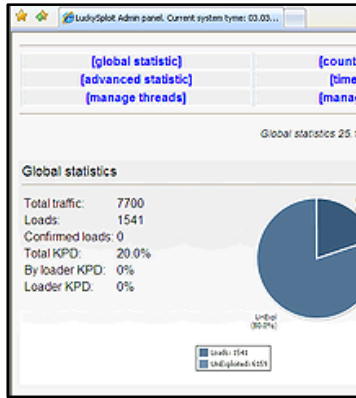
Malware Attack



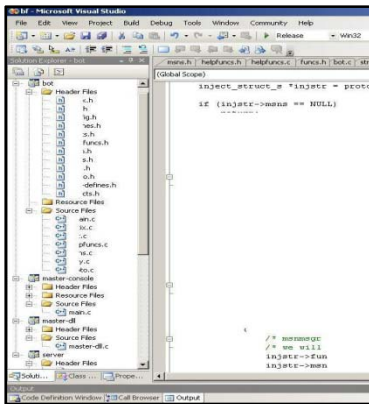
1. Nelle “dropzone” vengono collezionati i dati sottratti; nelle fasi preliminari viene effettuato il log del traffico HTTP dell’utente
2. Dalle informazioni ottenute l’attaccante studia le misure di sicurezza offerte dalla banca (modalità di autenticazione, alert lato utente, etc.)
3. L’attaccante crea una configurazione personalizzata per l’attacco



Malware for Luckysplot



URLZ



Bronze Edition



- Bu ürün Turkojan 3.0'da bulunan sorunların giderilip daha da geliştirildiği bir sürüm olup çeşitli kısıtlamalar içerir(Webcam görüntüsü,ses ve msn konuşmaları alınamamaktadır)
- Antivirüs programları ile sorun yaşanması halinde 1 ay boyunca yenisi ile değiştirme garantisi
- 7/24 e-mail vasıtasıyla teknik destek
- Windows 95/98/ME/NT/2000/XP desteği

Ürün Bedeli : 99\$ (Amerikan Doları) - 118.00 YTL

Silver Edition



- Antivirüs programları ile sorun yaşanması halinde 4 ay boyunca (en fazla 3 kez) yenisi ile değiştirme garantisi
- 7/24 e-mail ve anlık mesajlaşma sistemleri aracılığıyla teknik destek
- Windows 95/98/ME/NT/2000/XP/Vista desteği
- Webcam görüntüsü alabilme
- Clipboard değişikliklerini farkedip kaydedebilme

Ürün Bedeli : 179\$ (Amerikan Doları) - 214.00 YTL

Gold Edition



- Antivirüs programları ile sorun yaşanması halinde 6 ay boyunca(sınırsız) ya da 9 ay boyunca (en fazla 3 kez) yenisi ile değiştirme garantisi (seçimlik olarak kullanılabilir)
- 7/24 e-mail ve anlık mesajlaşma sistemleri aracılığıyla teknik destek
- Windows 95/98/ME/NT/2000/XP/Vista desteği
- MS-DOS komutları kullanabilme
- Webcam görüntüsü,ses ve msn loglarını alabilme
- Uzak bilgisayarı klavye ve mouse ile kontrol edebilme
- Clipboard değişikliklerini farkedip kaydedebilme
- Kurulum ve sonrasında birebir destek
- Uzak bilgisayardaki resimleri download etmeden görebilme

Ürün Bedeli : 249\$ (Amerikan Doları) - 300.00 YTL

er infettare i
er vulnerabili
a 500 dollari

te bancario
1000 dollari
di subscription



Data collection and analysis

■ Analisi delle informazioni collezionate

- ▶ L'attaccante cercherà di conoscere come l'applicazione bancaria funziona
- ▶ La seguente configurazione permette di analizzare il traffico HTML direttamente dal PC dell'utente:

```
ghjfe87=0  
hgknc87=*secure.newbank.com  
hgknn87 = <html>
```

- ▶ Le pagine HTML diventano decine di migliaia. Questo facilita un attaccante nel conoscere le funzionalità presenti su portali sconosciuti
- ▶ Recent analysis of Torpig, shows the same approach



Regole Personalizzate

■ Custom HTML injection (Silent Banker)

```
[jhw144]
pok=insert
qas=secureportal.bank.cm/index.do
dfr=16
req=100
xzq=9
rek=<input type="hidden" name="username_phish" value="">
<input type="hidden" name="password_phish" value="">
njd=name="login_Form"
xzn=value="">
```

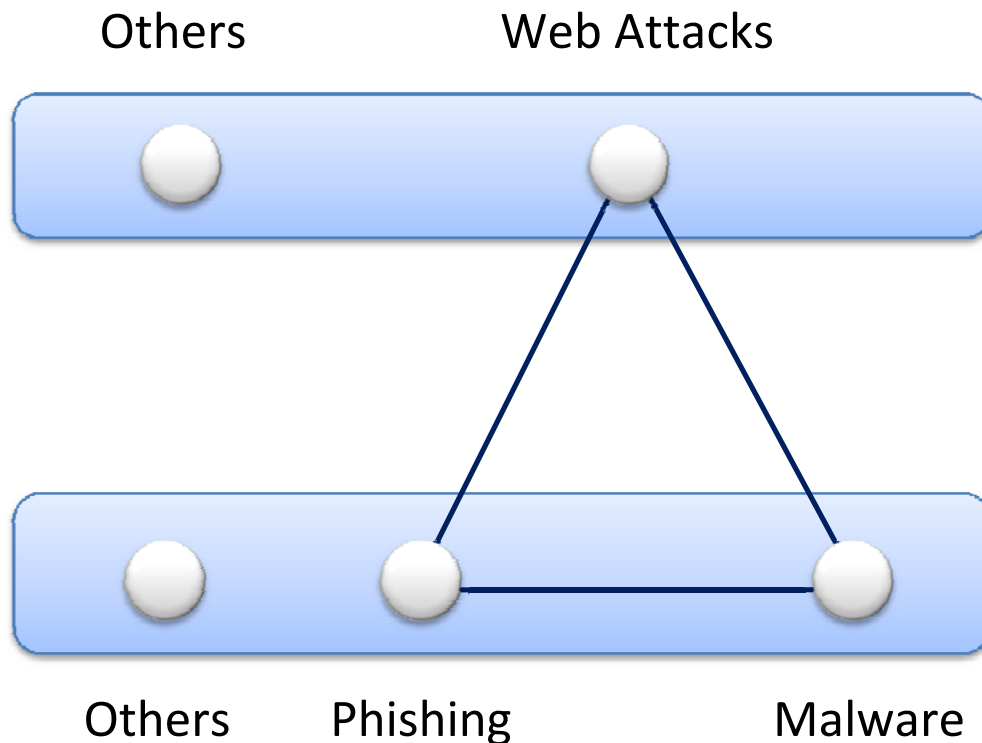
La precedente configurazione istruisce il malware ad utilizzare la string *“login_Form”* come riferimento, poi inserirà il contenuto in *“rek”* dopo il successivo *value="">*



Interazioni

■ Reciproco Potenziamento

- Gli attacchi diretti verso l'infrastruttura accrescono il potenziale degli attacchi verso gli utenti e vice-versa

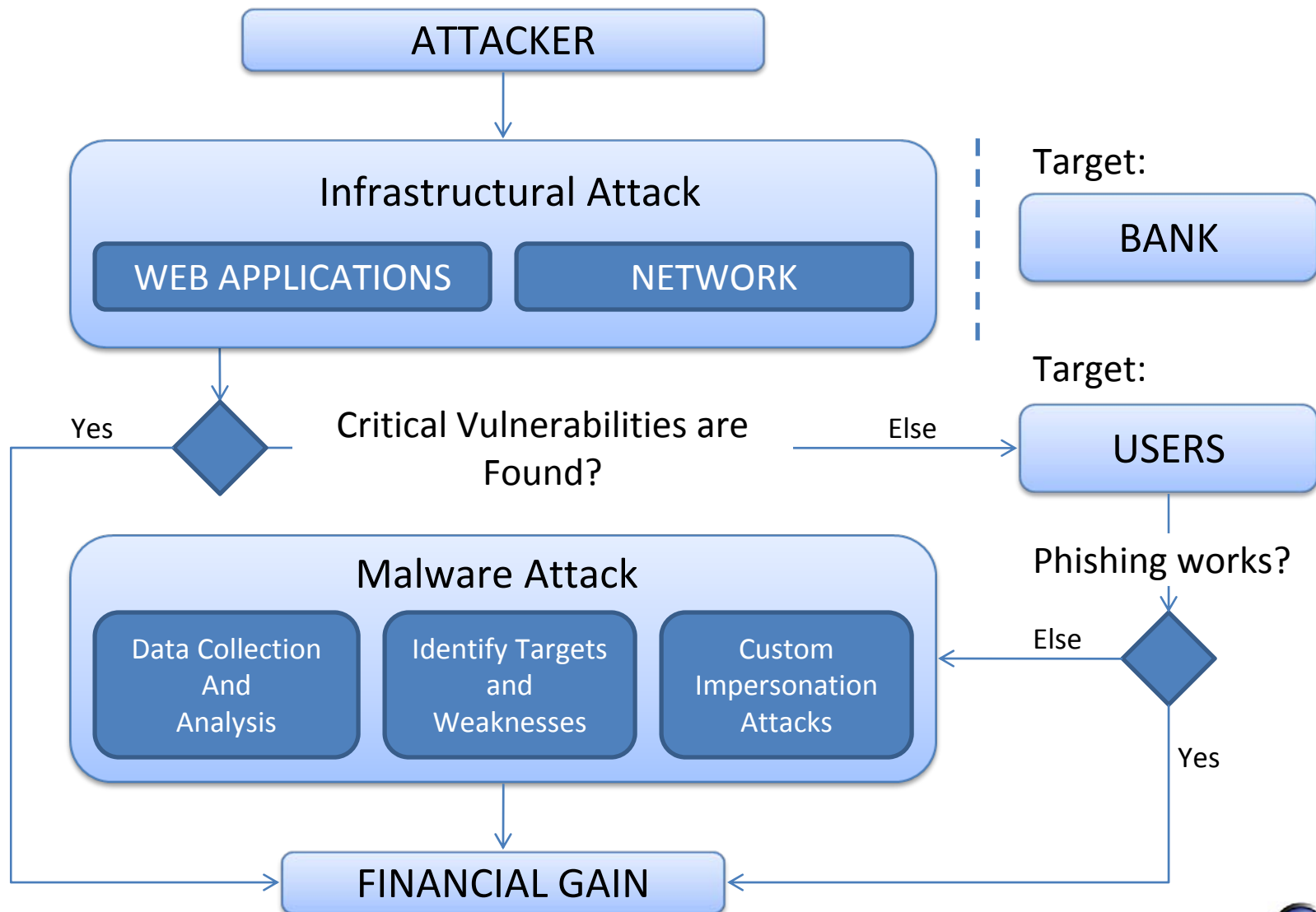


Attacchi
infrastrutturali

+

Attacchi contro
gli utenti

Processo di attacco



Malware e ritorno di investimento

Zeus and Nethell Dropzones

Information Category	Number	Percentage
Credit Cards	5682	3,44
Paypal	5000	3,02
Bank Accounts	5200	3,15
Email Passwords	149458	90,39

Rif: Holz, Engelberth, Freiling - Learning more About the Underground Economy

Silent Banker Dropzone

Information Category	Number	Percentage
Credit Cards	1120	6,35
Bank Accounts	865	4,91
Paypal	220	1,25
Email Passwords	15430	87,5

Rif: Owasp Antimalware

Torpig Dropzone

Information Category	Number	Percentage
Paypal	1170	1,84
Bank Accounts	6600	10,39
Credit Cards	1160	1,83
Email Passwords	54590	85,94

Rif: Stone, Cavallari, Vigna and others

Your Botnet is My Botnet: Analysis of Botnet takeover



Come proteggersi?

- Pre SDLC
- Define and Design
- Development
- Deploy And Maintenance



Pre SDLC

Define and Design



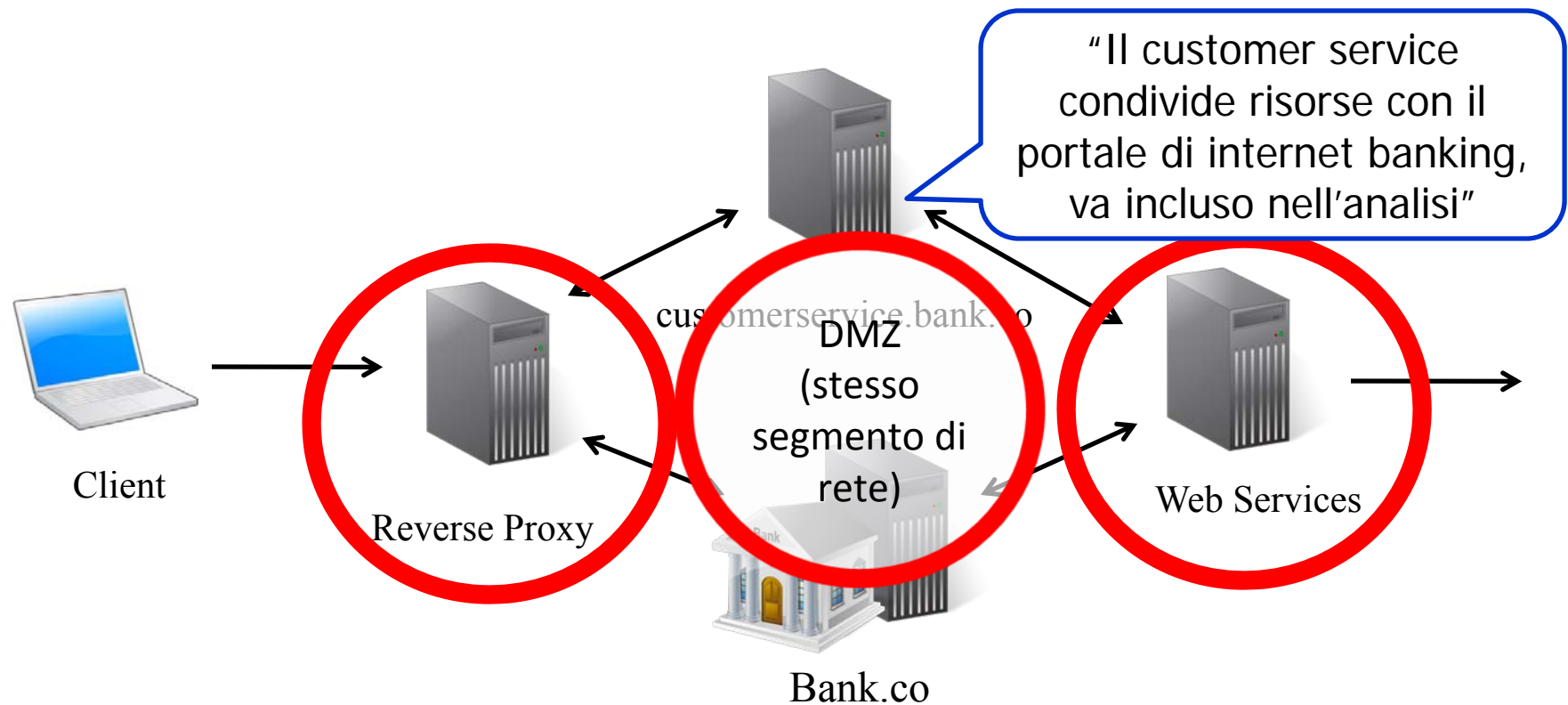
Primi step nella messa in sicurezza

- Dare la giusta priorità agli interventi
 - ▶ Overview dell'infrastruttura in senso ampio
 - ▶ Threat Modeling e Risk Rating
- Comprendere quali requisiti di sicurezza adottare
 - ▶ Analisi di settore
- Valutare le soluzioni prima dell'adozione
 - ▶ Solution Selection
 - ▶ Valutare i costi e benefici dei futuri investimenti tecnologici nel modo più oggettivo possibile



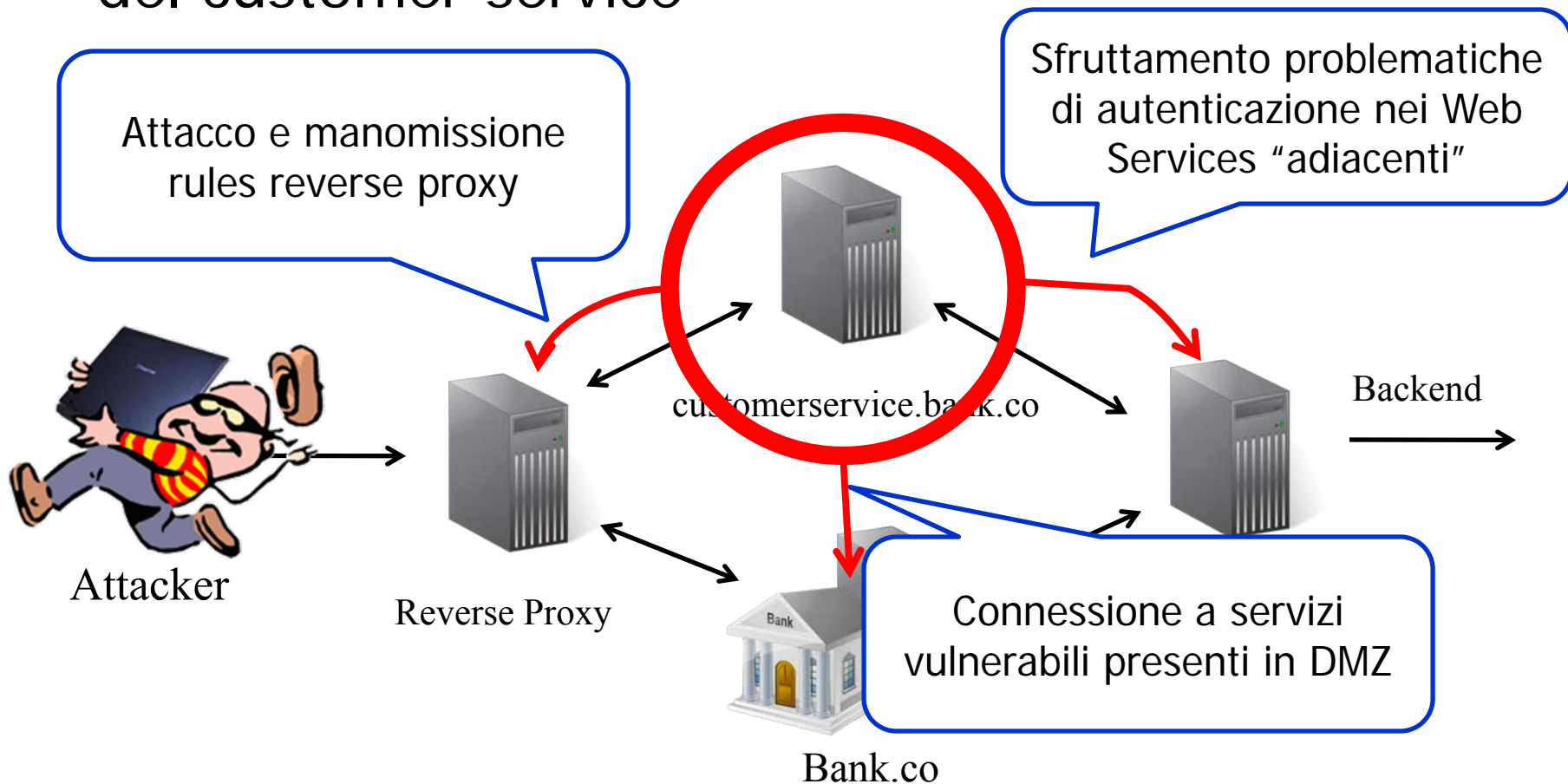
Estensione del perimetro di analisi

- La condivisione di risorse fra elementi differenti dell'infrastruttura è un punto di attenzione



Estensione del perimetro di analisi (2)

■ Potenziale di Attacco in caso di compromissione del customer service



Estensione del perimetro di analisi (3)

- Individuare dove il portale di internet banking interagisce con contenuti di terze parti
- Un attaccante potrebbe compromettere il portale *passando da un fornitore*



Includere Javascript esterno in modo dinamico è un rischio:

```
<!-- BEGIN Marketing Tag. PLACE IT BEFORE THE /BODY TAG -->  
<script language='javascript' src='https://www.unsafeagency.com/bank.com.js' >  
<!-- END Marketing Tag. -->
```

Definire le aree con maggior priorità

- Necessità di individuare *dove* siano presenti i maggiori rischi
- Assessment “rapido” e preciso
 - ▶ Assessment Network e Web
 - ▶ Black-Box o Grey Box
- Creazione di un cruscotto con i rischi infrastrutturali associati
 - ▶ In base ai rischi si vanno a delineare le priorità di intervento, su quali applicazioni e processi investire maggiormente in sicurezza



Definizione dei requisiti

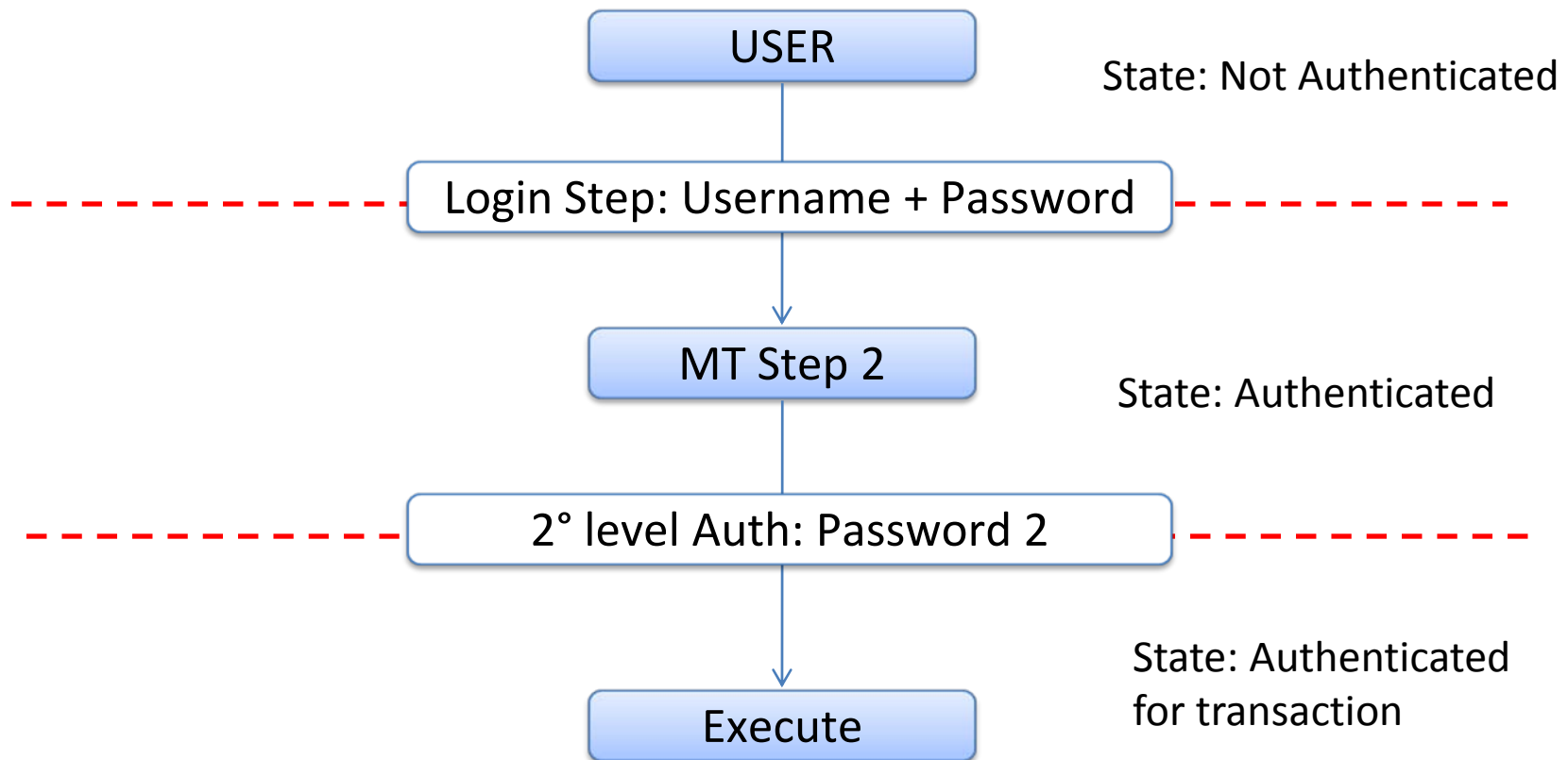
- Fase preliminare per la messa in sicurezza di una applicazione
 - ▶ Definire i requisiti di sicurezza
 - ▶ Definire dove questi requisiti debbano essere presenti
- Le scelte effettuate in questa fase difficilmente possono essere cambiate a posteriori
 - ▶ Esempio: scelta delle modalità di autenticazione



Trust Boundaries

Applies to:
corporate.bank.cm

- Identificare dove applicare le modalità di autenticazione scelte




Solution Selection

- ▶ Password



- ▶ TAN (Gridcard, Scratch Card)

- Transaction Authorization Numbers



	A	B	C	D	E	F	G
1	1234	1234	1234	1234	1234	1234	1234
2	1234	1234	1234	1234	1234	1234	1234
3	1234	1234	1234	1234	1234	1234	1234
4	1234	1234	1234	1234	1234	1234	1234
5	1234	1234	1234	1234	1234	1234	1234
6	1234	1234	1234	1234	1234	1234	1234
7	1234	1234	1234	1234	1234	1234	1234

- ▶ OTP (Time Based, Click)

- One Time password

- ▶ CAP (Random Challenge Response)

- Card Random Nonce is like OTP



- ▶ SIM card changes

- ▶ Cellphone Caller ID

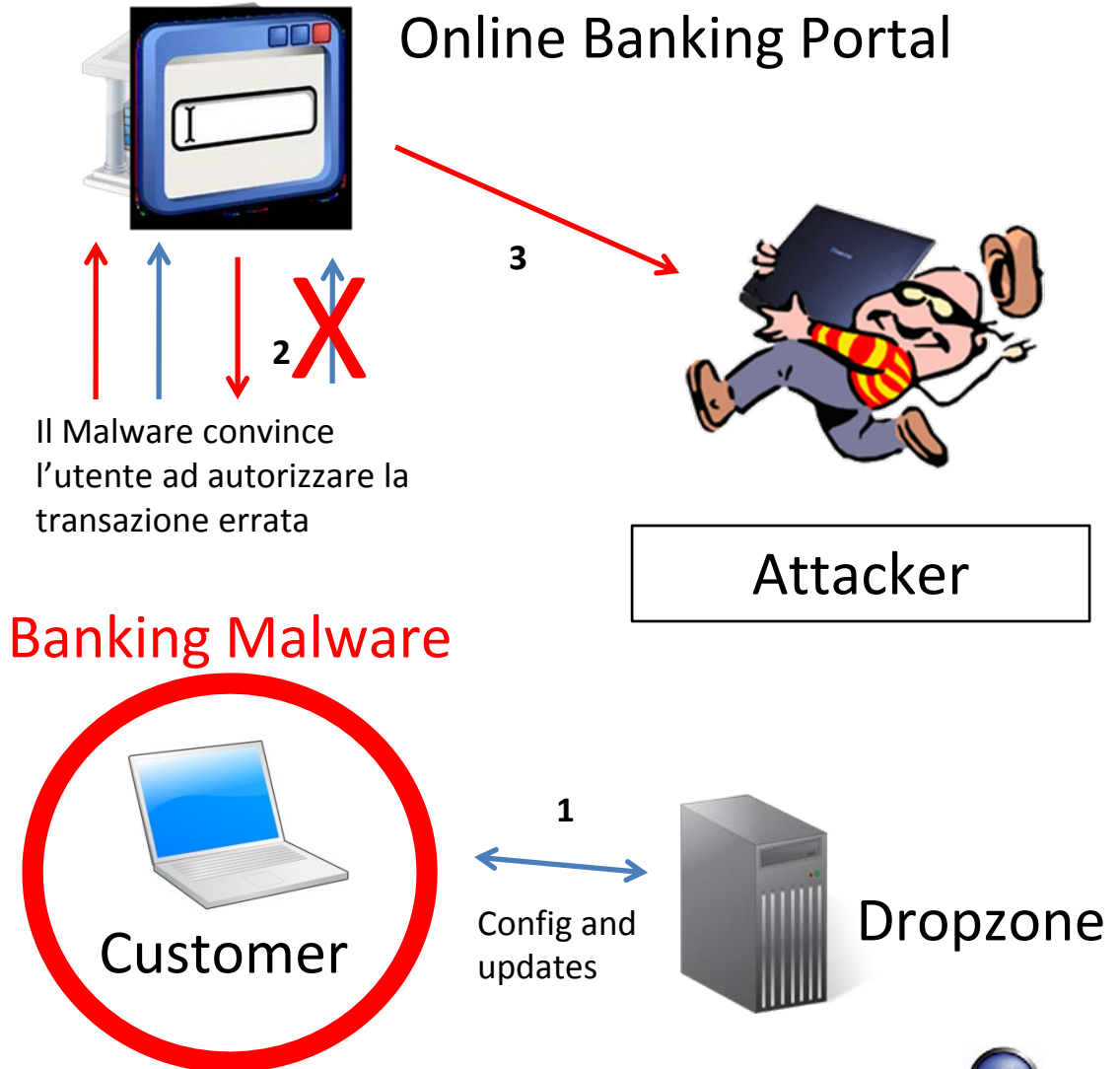


VULNERABILI AGLI ATTACCHI MALWARE

Silent Banking e Social Engineering

Qui è dato come presupposto che il computer dell'utente sia infetto.

- 1) L'attaccante costantemente aggiorna le definizioni per un alto numero di banche
- 2) Quando un utente effettua una transazione, il malware chiede il codice corretto e sostituisce i dettagli della transazione
- 3) L'utente autorizza una transazione differente



Solution Selection (2)

■ E' importante valutare i costi vs benefici, ovvero quale è l'incidenza?:

▶ In Italia circa 1/5 delle macchine sono infette

- Di queste solo 1/10* sono infette da un Trojan Stealer e/o Trojan Banker

- Di queste infezioni solo 1/10* operano contro le autenticazioni a più fattori proprie della banca usata dall'utente

- » = 2 utenti su Mille!

■ Oltre alle precedenti esistono soluzioni progettate in modo specifico per contenere i Malware

■ Esistono operazioni di contenimento che possono rafforzare le misure esistenti



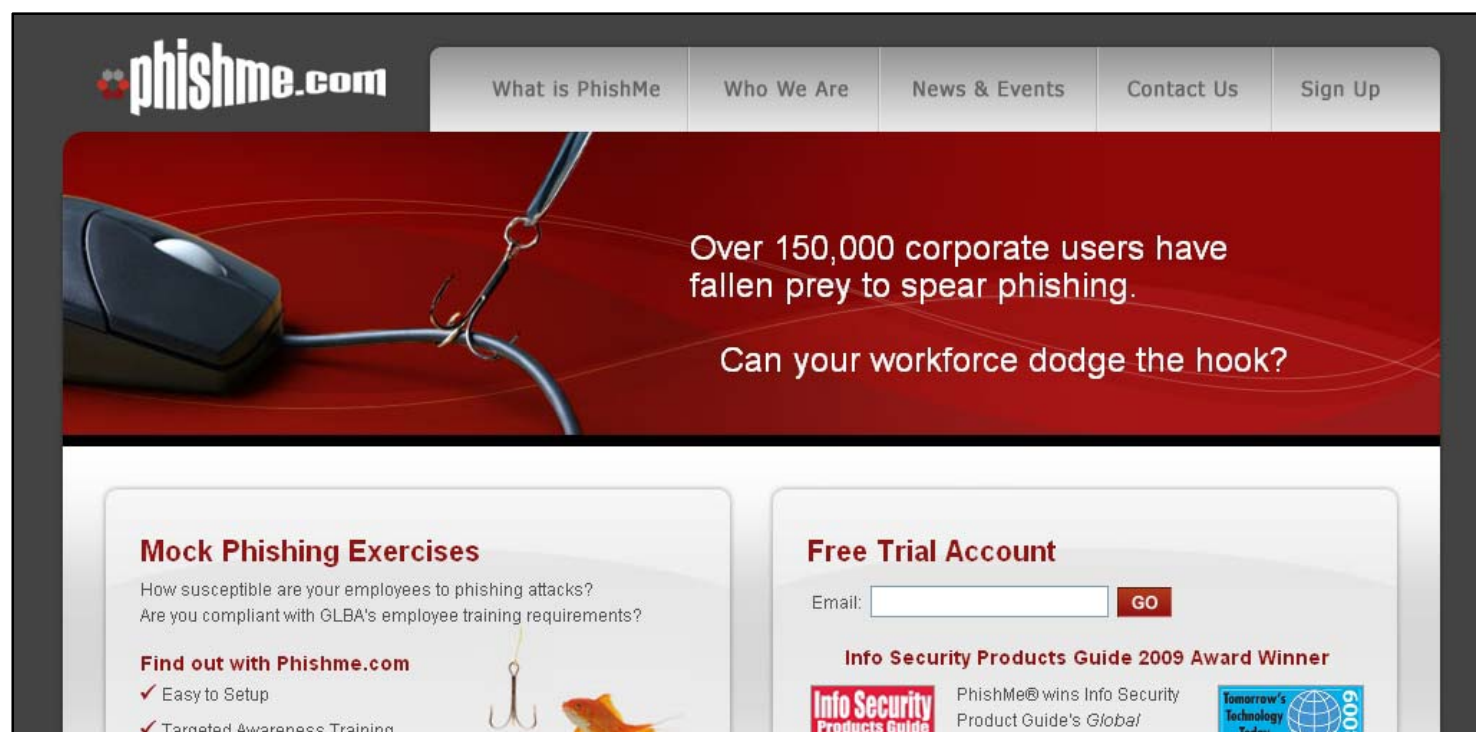
Metodi di contenimento

- Rinforzare l'informativa verso l'utente
 - ▶ Indicazioni costanti dei movimenti
 - ▶ Utilizzando possibilmente canali differenti (es. SMS)
 - ▶ Proteggere la possibilità di disabilitare queste funzioni
- Una transazione fraudolenta può essere bloccata se individuata in tempi rapidi
- L'informativa addizionale è importante, poiché il saldo via Web può essere "ricomputato"



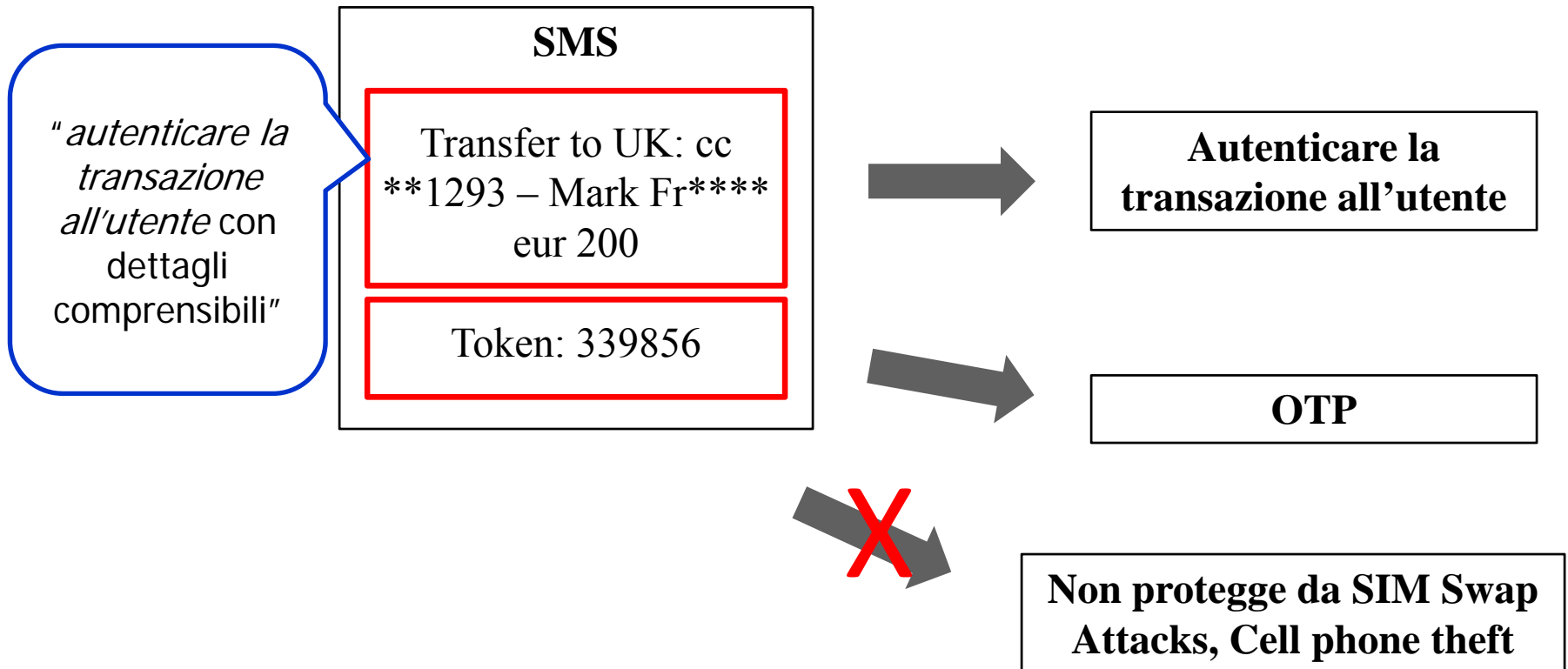
Metodi di contenimento (2)

- Awareness e training
- Meglio se effettuato nel tempo utilizzando test case reali



SMS challenge + Informativa

- Esempio di soluzione di contenimento, mantenendo modalità pre-esistenti



Development e Deployment

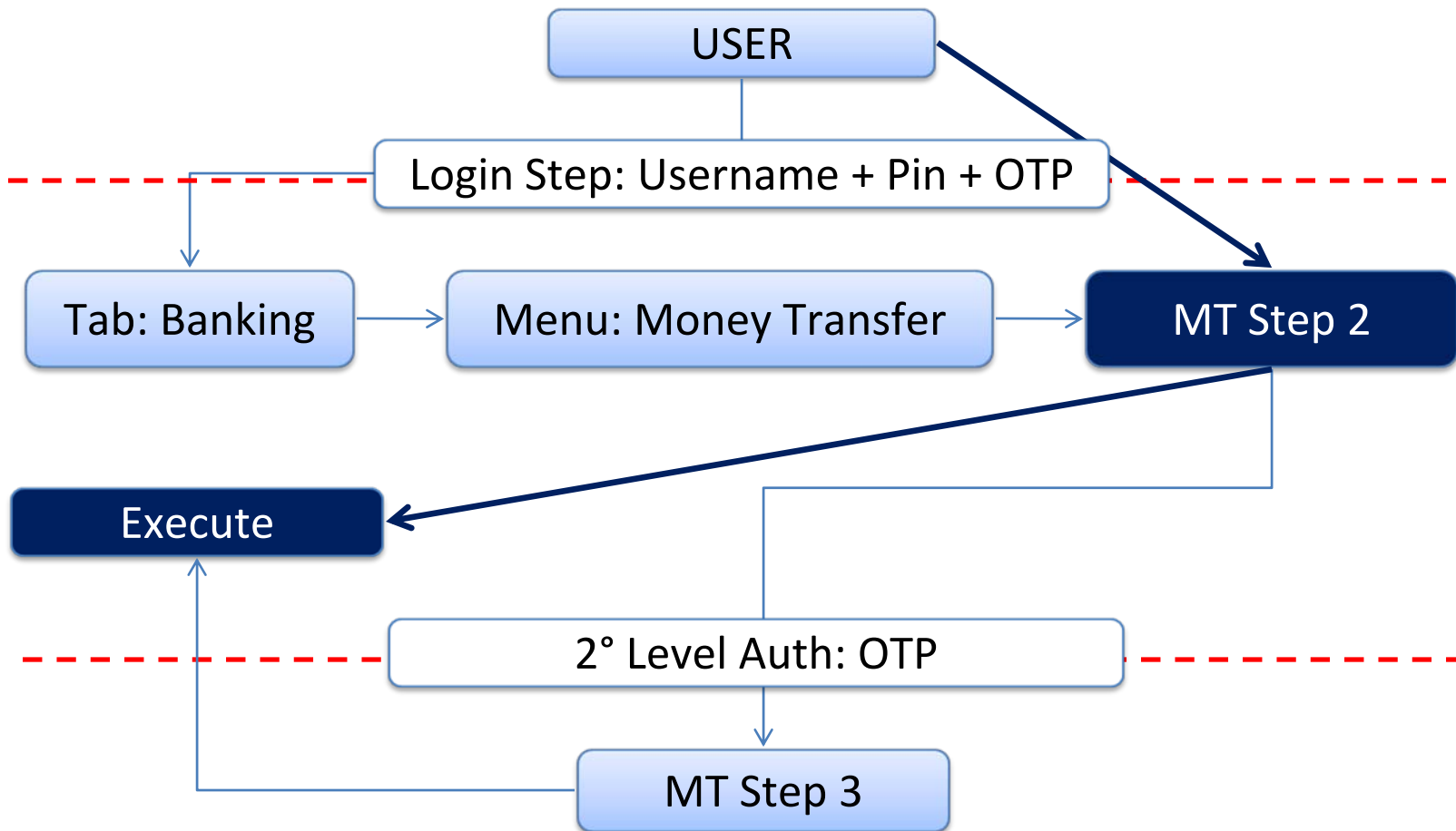


La sicurezza nello sviluppo è fondamentale

- Il secure design non protegge l'applicazione dalle vulnerabilità inserite nella fase di sviluppo



Es. Broken Access Control su funzionalità dispositiva



Problematiche costanti nella fase di sviluppo

■ Broken Access Control in lettura

- ▶ Passando il numero di conto si accede ai dati di quel conto, senza verificarne l'appartenenza
- ▶ Estratto conto in PDF, se l'ID è corretto viene restituito il file PDF senza verificarne l'appartenenza

■ Uso di funzioni pericolose

- ▶ Esecuzione di codice in modo dinamico → Eval()
server side

■ Errori nella gestione del Session State

- ▶ Problematica del "Back Home"



Problematiche costanti nella fase di sviluppo

■ Upload di file

- ▶ Le funzionalità di upload permettono spesso di poter creare file con estensioni arbitrarie → Code Execution

■ Creazione insicura di file

- ▶ Possibilità di sovrascrivere un file esistente → Code Execution

■ Path Traversal

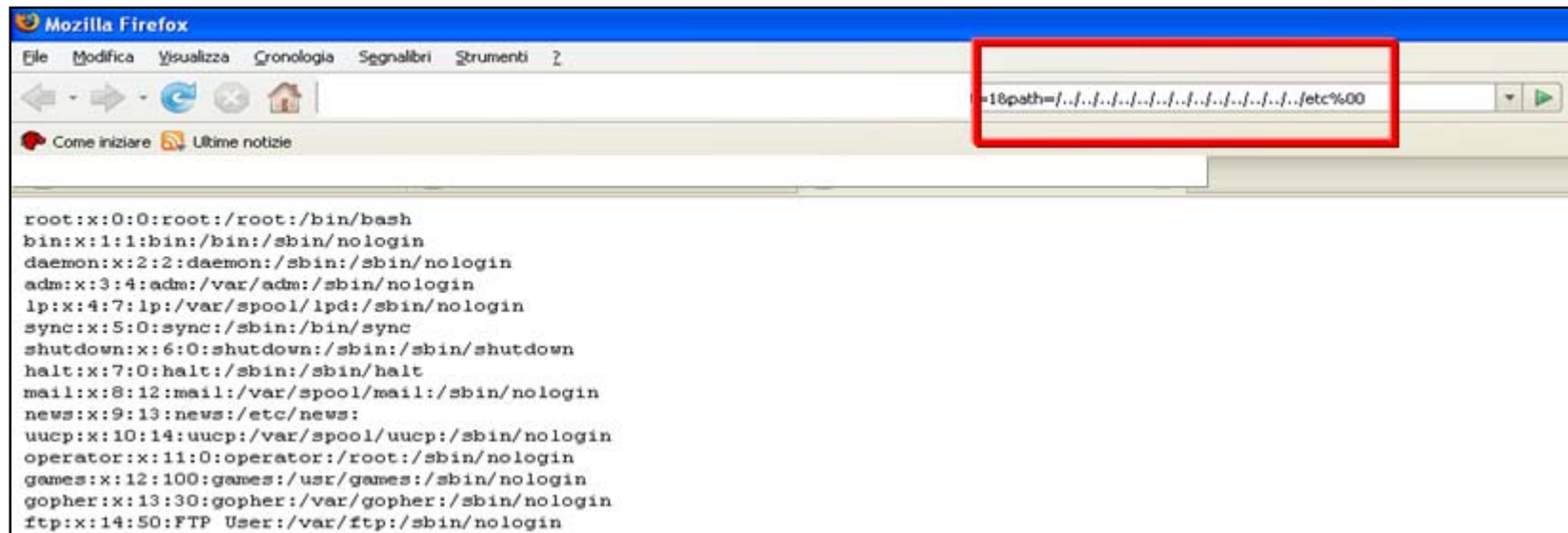
- ▶ Possibilità di leggere file arbitrari, specificando una risorsa posta ad un livello inferiore



Path Traversal

Path Traversal ed accesso in lettura a file arbitrari:

<http://www.sito-.com/sito/download.jsp?id=../../../../../../../../etc/passwd%00>



```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```



Es. di Cross Site Scripting

Il campo di ricerca
riporta le parole
ricercate a video.

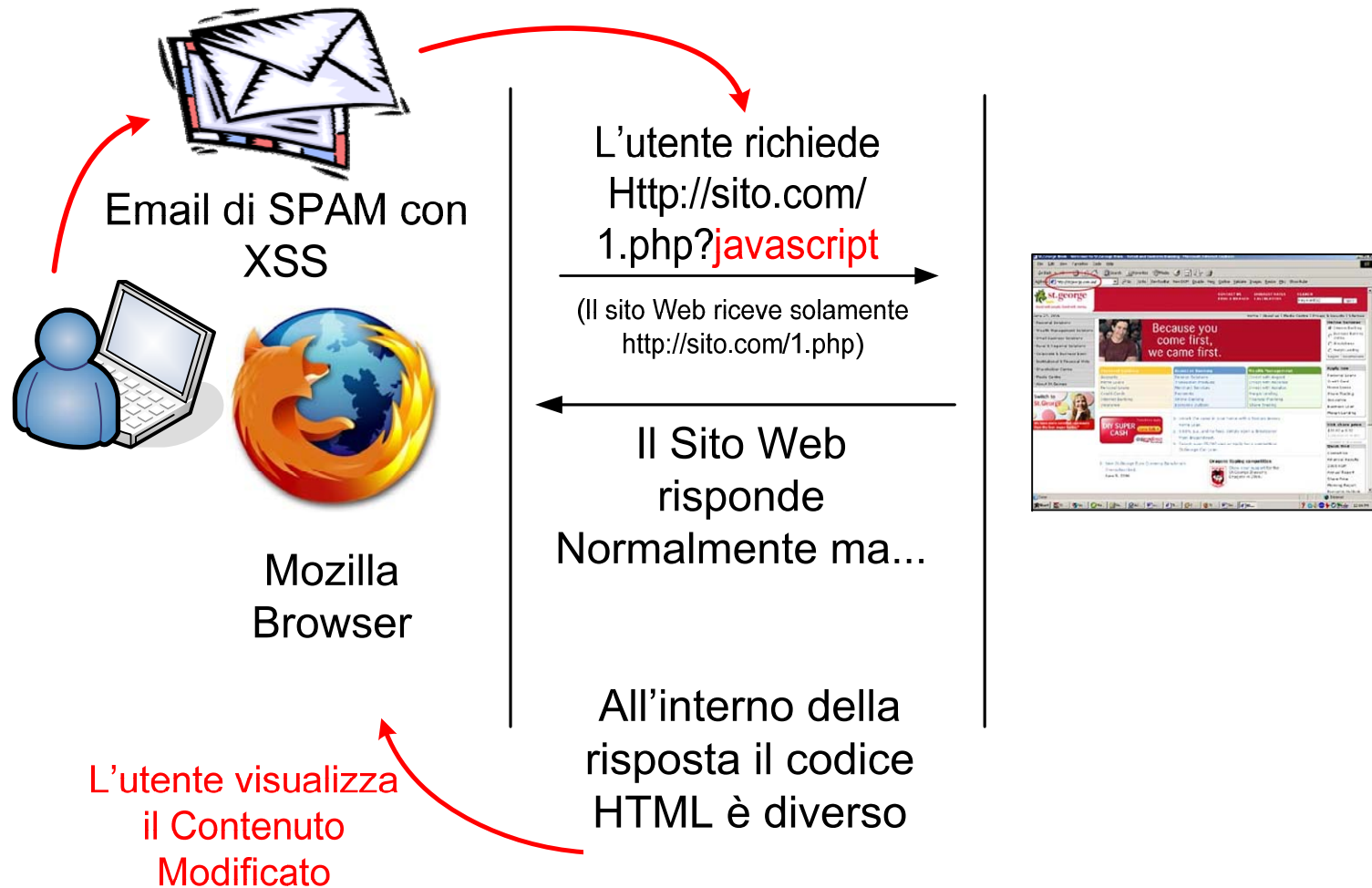
Cerco: `<script>alert(document.cookie)</script>`



Il sito invia lo script
all'utente e visualizza
un cookie di sessione
in una finestra di pop-
up.



Attacco di Phishing tramite XSS



Problematiche di configurazione

■ Interfacce di Management Esposte

- ▶ Possibilità di esecuzione di codice o di inserimento di contenuto permanente nel caso in cui sia possibile accedervi

■ Open Proxy

- ▶ Un reverse proxy configurato come proxy standard, può consentire l'accesso a risorse interne

■ Contenuti protetti da URL Rewriting

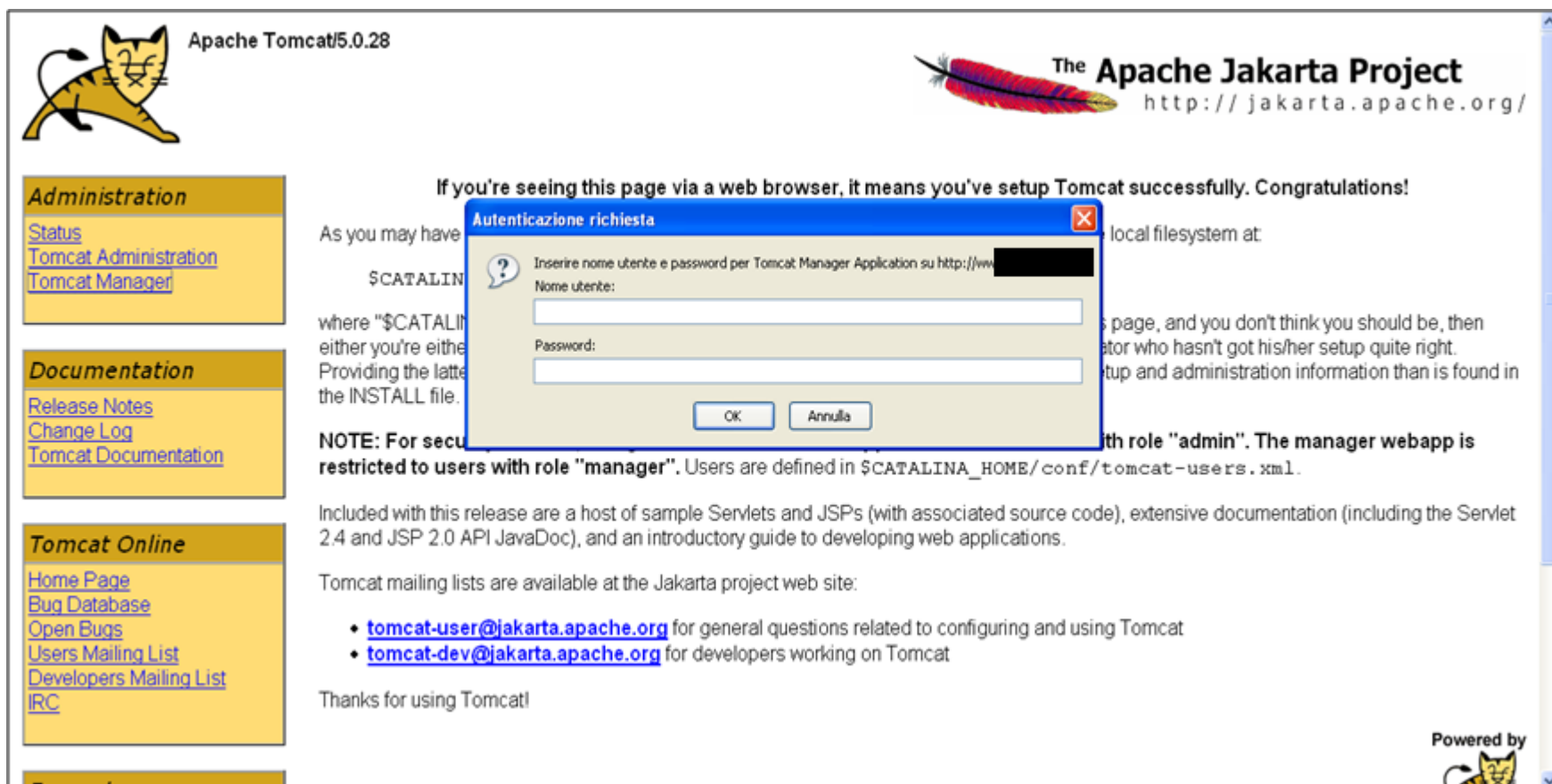
- ▶ Possibilità spesso di bypassare la protezione tramite appropriati encoding



Contenuti protetti da URL Rewriting

Double Encoding, utile per ingannare i filtri

Es: <http://www.sito-.com/sito/%252e%252e/>



The screenshot shows the Apache Tomcat 5.0.28 installation success page. The page features the Apache Tomcat logo (a cat) and the Apache Jakarta Project logo (a feather). The main text reads: "If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!". Below this, there is a section for "Administration" with links to "Status", "Tomcat Administration", and "Tomcat Manager". There is also a "Documentation" section with links to "Release Notes", "Change Log", and "Tomcat Documentation". A "Tomcat Online" section contains links to "Home Page", "Bug Database", "Open Bugs", "Users Mailing List", "Developers Mailing List", and "IRC".

An authentication dialog box titled "Autenticazione richiesta" is overlaid on the page. It contains the text: "Inserire nome utente e password per Tomcat Manager Application su http://www. [redacted]". It has two input fields labeled "Nome utente:" and "Password:", and two buttons labeled "OK" and "Annulla".

The page also includes a "NOTE: For security reasons, the manager webapp is restricted to users with role 'manager'. Users are defined in \$CATALINA_HOME/conf/tomcat-users.xml." and a list of mailing lists: "tomcat-user@jakarta.apache.org" for general questions and "tomcat-dev@jakarta.apache.org" for developers working on Tomcat.

Parameter Tampering

- Problematica comune di configurazione
 - ▶ Simile alla “Positive Authentication”
 - ▶ Identificabile facilmente se vengono protetti esplicitamente SOLO alcuni metodi
 - ▶ Avviene solitamente quando l'applicazione ha un unico utente ed il controllo di accesso viene fatto sul metodo
- METODI HTTP → GET, POST, HEAD...
- METODI INESISTENTI → GIO, METHOD, ...





Questions

**OWASP
Day IV**

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>