ISACA
Rome Chapter

Incident Response Experience

Round-up sugli attacchi informatici più recenti e sulle attività di mitigazione attuabili

Stefano Maccaglia
Chief Research Officer
Black Sun Labs

Agenda

- Introduzione all'Incident Response nel 2013.
- I nuovi rischi.
- Le difficoltà della forense post incidente.
- L'analisi degli Exploit Kit.
- Alcuni casi di esempio

L'Incident Response nel 2013

- Saper gestire un malware è un elemento critico in ogni incidente di Sicurezza.
- La Malware Analysis inizia con la forense e termina con il report fornito all'Incident Manager.
- L'attività coinvolge gli analisti forensi, gli analisti dei malware e gli analisti di rete.
- Solo attraverso l'analisi del codice malizioso, e l'identificazione delle modalità di infezione, propagazione e interconnessione con le strutture esterne diventa possibile comprendere quali logiche hanno armato i cybercriminali.

L'Incident Response nel 2013

- Alcune organizzazioni (Mandiant, per esempio) hanno sviluppato un set di indicatori che può aiutare a derivare le informazioni essenziali di ogni compromissione in modo da identificare gli artefatti malevoli presenti all'interno di una rete aziendale.
- In ogni caso, per la mia pluriennale esperienza di Incident Response Team Leader, il processo è sempre molto più complesso ed è fortemente influenzato dalla tipologia di attacco attuato e dall'organizzazione e la capacità reattiva della compagine aziendale.

Le problematiche della forense nell'IRT

- Ormai non è più possibile attuare una Response esclusivamente reattiva pena il rischio di mancare numerose situazioni critiche.
- La forense sta diventando sempre più complessa e inaffidabile, soprattutto a causa dell'innesco di nuove tecnologie per i Dischi (SSD) e per la crittografia dei Dati (…) nonché per le tecniche di offuscamento dei malware.
- La diffusione dei malware ha cambiato le meccaniche principali di diffusione spostandosi su vettori temporanei e difficilmente individuabili, soprattutto per la prima fase di attacco.
- I keylogger e gli stealer non necessitano più di restare persistenti.
- I malware più complessi sono in grado di persistere attraverso sistemi non noti.

Un esempio di analisi: Cool Exploit Kit

Cool Exploit Kit

- Il Kit è stato sviluppato in Russia, e i suoi exploits sono crittati con algoritmi privati e con IonCube (per la parte Web). Questo rende piuttosto difficile analizzare le infezioni innescate da Cool EK se non si hanno le capacità tecniche, i giusti Sistemi di deoffuscamento e una buona dose di pazienza.
- Il Kit usa Java OBE (Open Business Engine) e vulnerabilità Java per la sua diffusione massiva, ma offre anche exploit basati su .pdf e altre tecnologie.
- L'attacco è strutturato intorno al Drive-by Download.

Il Drive-by Download

- Se la vittima segue un Iframe malevolo o carica una pagina eseguendo il codice Java in essa presente, o ancora apre un file .pdf infettato, essa subirà uno o più tentativi di attacco basati su iniezione.
- Nel caso Java il vettore (Loader), alla sua esecuzione, scaricherà in memoria (senza scrivere su disco) dei comandi Java contenuti in un file JAR.
- Il file JAR contiene anche parametri URL codificati che verranno decodificati opportunamente da una specifica classe Java.
- Alla sua esecuzione il file JAR decodificherà il/i parametri per avere una URL in clear text.
- Questa URL permetterà di scaricare ed eseguire ulteriori payload maliziosi.

Cool Exploit Kit: Exploit as a Service (EaaS)

- Cool Exploit Kit è offerto in "affitto" o in modalità "acquistabile".
- I cybercriminali possono affittare il kit per 24 ore, una settimana o un mese pagando dai $40, ai $450 per il servizio.
- In termini di "innovazione" non c'è molto da rimarcare.
- Il kit è estremamente simile a Blackhole, ma la sua strategia di vendita è più vicina a un servizio che a un Kit malizioso .
- I "Clienti" possono scegliere come "personalizzare" le meccaniche di infezione (magari definendo uno specifico subset di macchine target da infettare) o possono richiedere agli sviluppatori di gestire per loro il "servizio" di injection.
- Gli "utilizzatori" dell'Exploit Kit ricevono notifiche quando i loro domini da cui pubblicano l'infezione iniziano ad essere inseriti nelle blacklist dei vari vendor antivirali e delle soluzioni di DNS IP Reputation.

L'Architettura del Kit

- In termini di architettura Cool EK, è composto di due essenziali componenti:
  - **Il sito web** dove configurare la funzione di **Injector**.
  - Il sito web dove amministrare le vittime (C&C) e attivare altri payload di secondo e terzo stadio.
- Tutti i componenti possono risiedere all'interno di una singola macchina. Spesso questa soluzione è usata su "Bulletproof server".
- La GUI amministrativa include i "Widgets".
- La maggior parte dei widgets offrono le informazioni già viste per altri Kit : statistiche, tipo di OS nei computer vittima, top country e referrer.

L'Injector

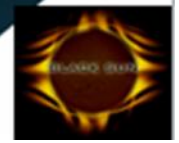
- L'injector di Cool Exploit Kit è estremamente pericoloso.
- Esso infetta il browser della vittima quando essa si connette al sito infettato, veicolando differenti exploit.
- A seguito di un exploit funzionante, l'Injector può attivare uno stealer minimale o può far caricare ulteriori payload maliziosi assicurandone anche la persistenza sul computer vittima.
- A livello basilare Cool, come Blackhole, è una sorta di Framework per trafugare informazioni o assicurare infezioni massive di grande impatto per strutture pubbliche, ma anche a danno di aziende specifiche (attraverso attacchi di tipo "spear phishing" o ". La differenza è limitata al tipo di tattica adottata dai cybercriminali..

Gli obiettivi dell'Injector

- Quale che sia il metodo usato per spingere l'utente a interagire (Drive-By) con il sito malizioso contenente l'Injector, gli obiettivi di quest'ultimo sono:
  - Catturare i parametri inclusi nell'URL lanciata. Questo permette all'Exploit Kit di correlare la pagina richiesta con lo specifico individuo responsabile del redirect (per le statistiche e per il pagamento, in alcuni casi).
  - Identificare la macchina vittima. La pagina caricata attiva la richiesta dello User-Agent e di altri parametri del browser per identificare :
    - Sistema Operativo della Vittima
    - Browser (and browser version)
    - Versione di Adobe Flash
    - Versione di Adobe Reader
    - Versione di Java
  - In base a questi dati l'Injector scarica e attiva l'exploit adeguato (PDF, Flash, Java etc).
  - In caso di fallimento dell'exploit l'Injector inizia a far caricare un set di exploit fino all'infezione o al fallimento dell'attacco

La crittografia nell'Injector

- Per proteggere l'Injector da potenziali intercettazioni e blocchi operati da sistemi di difesa quali gli Antivirus, i coderz hanno sviluppato delle tecniche molto interessanti.
- La più diffusa verte sulla iniezione di una URL codificata all'interno di un Java o Javascript "contenitore" nel quale sono presenti le istruzioni necessarie al decode della URL e al suo caricamento.
- Questo meccanismo impone agli antivirus che volessero bloccare l'attivazione dell'Injector, di "conoscere" in anticipo le URL nascoste all'interno dei file o la perfetta configurazione dei file stessi.
- Per rendere più complessa questa operazione gli attaccanti inseriscono, in ogni Java generato dinamicamente dell'entropia rendendo questa possibilità non percorribile.



Cool Exploit Kit in Action

- Un classico messaggio di posta usato come vettore:

This message is to notify you that your package has been processed and is on schedule for delivery from ADP.

Here are the details of your delivery:
Package Type: [redacted]
Courier: UPS Ground
Estimated Time of Arrival: [redacted]
Tracking Number (if one is available for this package): [redacted]

Details: Click here to overview and/or change order

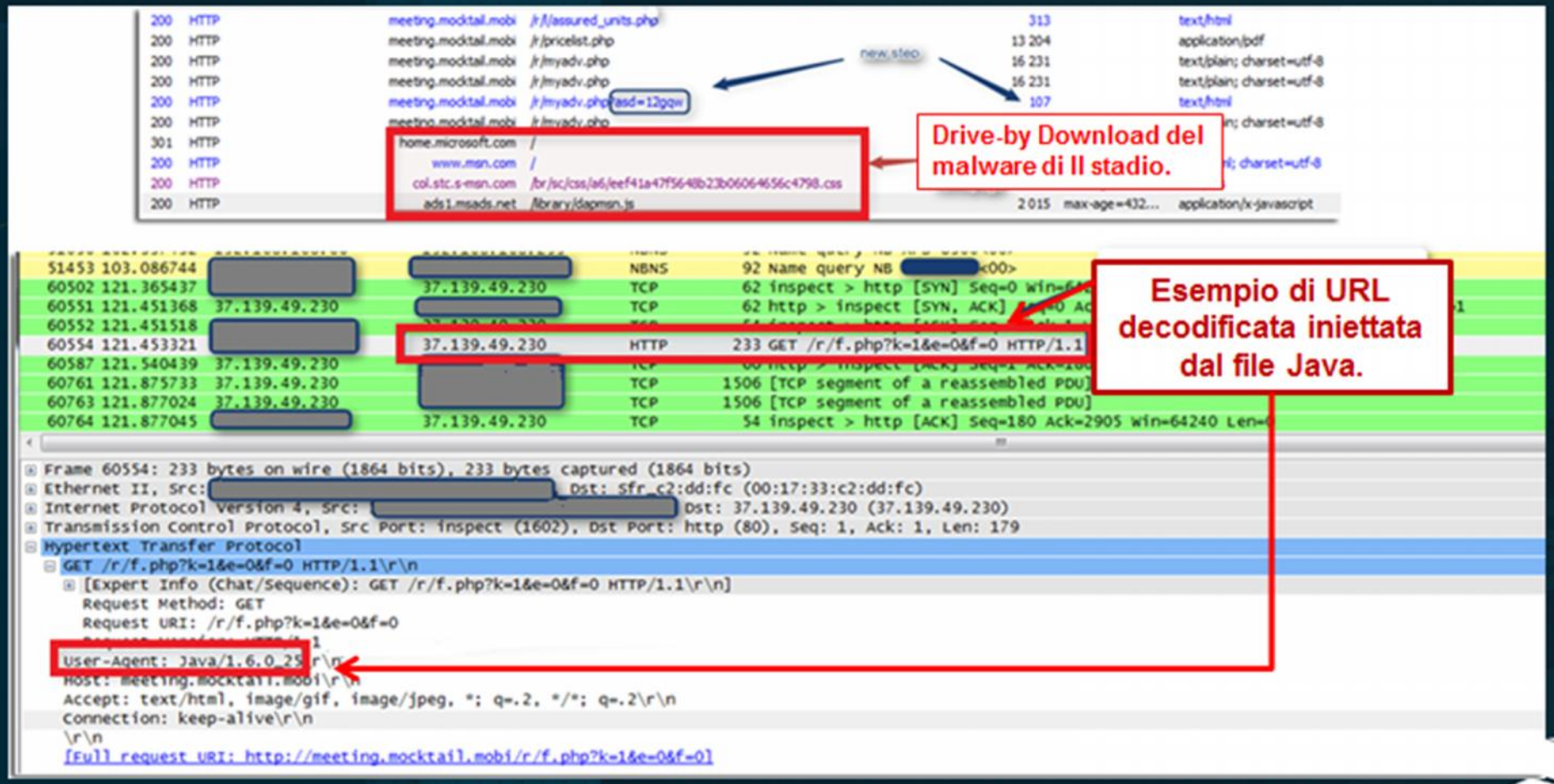
We will notify you via email if the status of your delivery changes.

Access these and other valuable tools at support.ADP.com:
o Payroll and Tax Calculators
o Order Payroll Supplies, Blank Checks, and more
o Submit requests online such as SUI Rate Changes, Schedule Changes, and more
o Downl oad Product Documentation, Manuals, and Forms
o Download Software Patches and Updates
o Access Knowledge Solutions / Frequently Asked Questions
o Watch Animated Tours with Guided Input Instructions

Thank You,
ADP Client Services
support.ADP.com

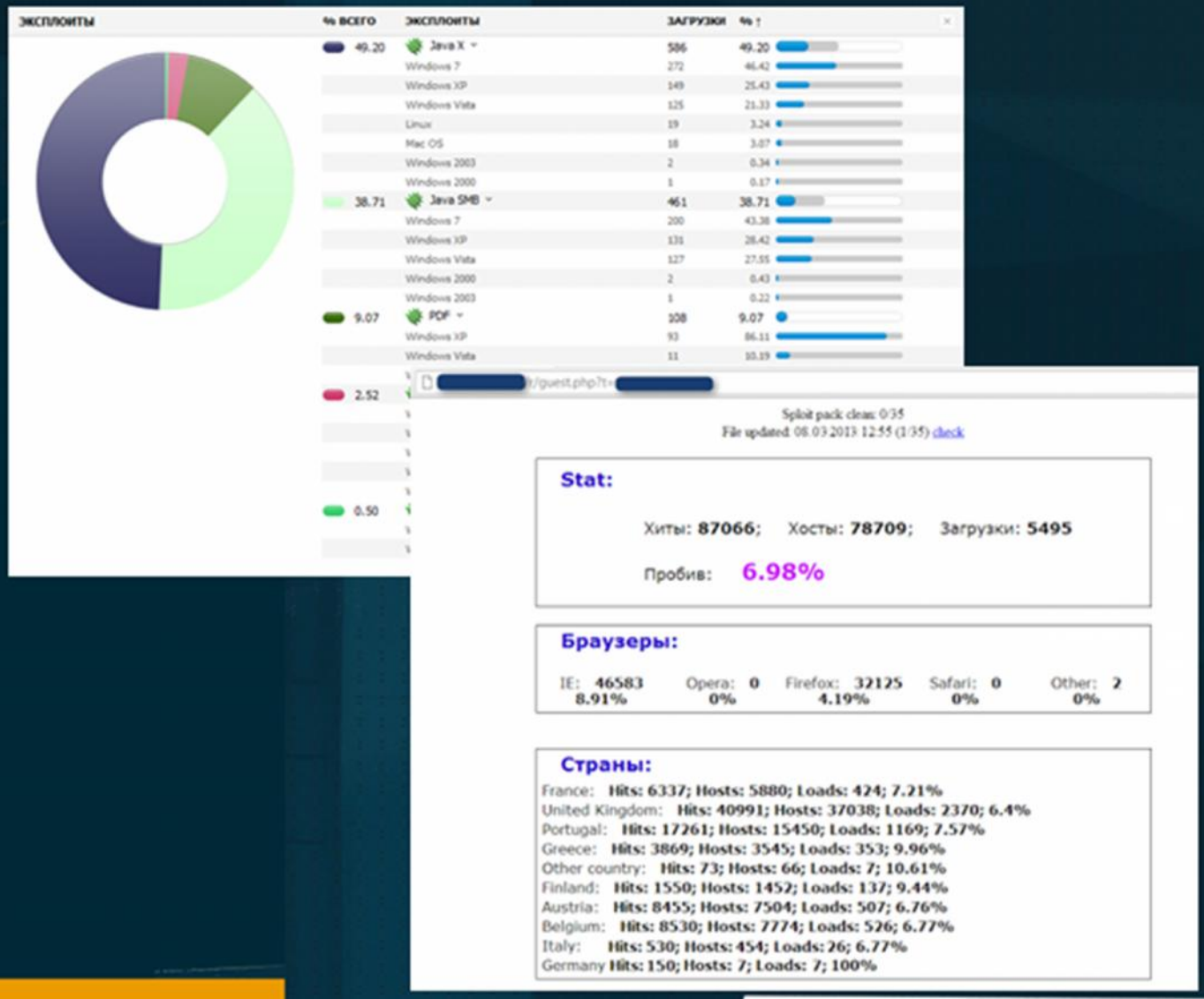
Cool Exploit Kit in azione

- L'injection dagli occhi del browser e dell'IDS



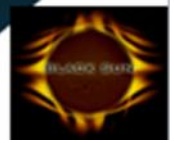
Cool Exploit Kit: Il pannello della C&C

- I widget di cui vi parlavo:



Cosa possiamo trovare di un Exploit Kit?

- Sono molto poche le tracce che gli Exploit Kit lasciano nel computer vittima.
- I payload veicolati direttamente sono crittati con meccanismi custom e predisposti per aggirare le logiche di ispezione degli AV e degli HIPS attraverso l'iniezione diretta in memoria. Inoltre, una volta iniettati non vengono scritti su disco e si cancellano al chiudere della sessione del browser.
- I payload di II livello sono di solito malware polimorfici crittati e compressi con sistemi specifici. Tipici esempi includono:
  - Fake AV (scareware)
  - Zeus
  - TDSS rootkit
  - ZeroAccess rootkit
  - Ransomware



Le azioni preventive

- Per impedire infezioni veicolate via Exploit Kit, e più in generale Drive-by, occorre identificare le pagine dell'Injector.
- Ma questo non è facile, perché impone ispezioni puntuali alle pagine caricate dal browser delle vittime. Appena una nuova pagina viene usata, tale pagina non sarà identificabile.
- Lascio di seguito esempi di pagine di Injection legate a Blackhole EK:
  - [removed]/google.php?gmpid=2a4baa70301068 62
  - [removed]/check.php?uid=42c1be945fc07c4b
  - [removed]/main.php?page=c9588fff43ed343a
- Queste pagine hanno un'apparenza assolutamente innocua. L'unico elemento che permetteva l'identificazione, una volta deoffuscate era la presenza di un parametro caratteristico: "StatParamName", ma si sono dovute svolgere molte analisi per scoprirlo.

L'analisi delle pagine

- Una volta scoperto quel parametro si è potuto identificare un ulteriore subset di pagine contenenti l'Injector:
  - [removed].in/t/a92b21c45c3ef0827e3dcf9c20972ec7
  - [removed].ftp1.biz/t/eb6d7764d6d6df02ed22a227a03b9f91
  - [removed].ddns.info/t/1baed7122e877523eb375daf0ffc45e6
  - [removed]/w.php?f=b6863&e=0
  - [removed]/w.php?f=19&e=1
- Queste pagine sono state usate da un altro server e contenevano un Injector simile alle pagine identificate in prima istanza.
- Resta da notare che questi due attacchi sono stati perpetrati a danno di uno stesso Cliente Corporate, in uno stesso periodo, da cybercriminali appartenenti a organizzazioni diverse…

ISACA
Rome Chapter

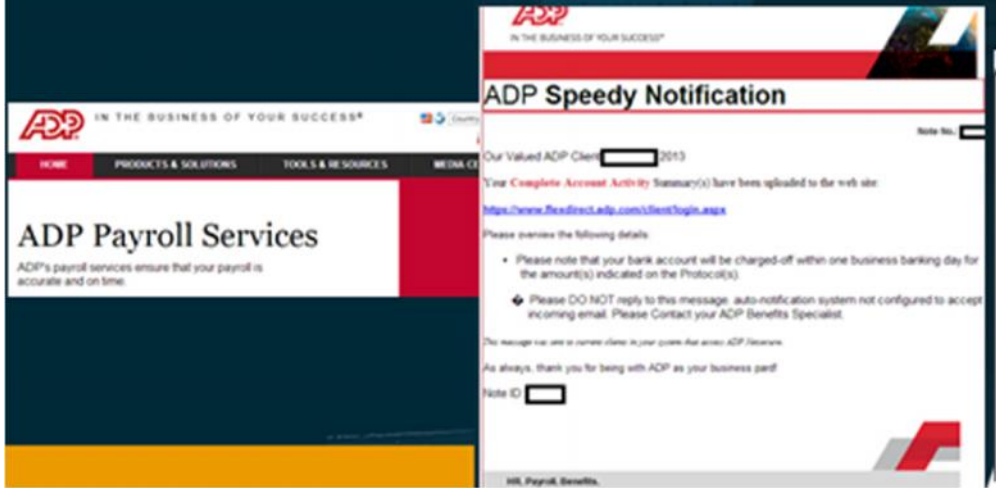
Attacchi Mirati:
CVE-2013-0633 e CVE-2013-0634

Attacchi mirati

- Gli attacchi di questo tipo non si limitano a infezioni massive, ma possono essere attuati anche in una logica "mirata".
- E' il caso identificato lo scorso Febbraio e che ha colpito il settore Aerospaziale attraverso l'ausilio di un due vulnerabilità Zero-Day diffuse negli "ambienti" dell'underground asiatico.
- Queste vulnerabilità sono state sfruttate per tentativi di spionaggio industriale.
- Le meccaniche di infezione sono molto vicine a quelle degli Exploit Kit e del Drive-By, ma sono state sfruttate in una logica puntuale usando liste di utenze e di aziende specifiche a cui tentare di propagarli, differentemente a quanto si fa nel caso degli attacchi massivi.

CVE-2013-0633 e CVE-2013-0634

- Le vulnerabilità indicate nel titolo sono state sfruttate proponendo alle vittime link via messaggi di tipo "spear phishing".
- I bersagli sono state numerose aziende aerospaziali, soprattutto dell'Occidente.
- Ona di queste email conteneva un documento Word chiamato *"2013 IEEE Aerospace Conference schedule"*, e un altro riportava informazioni su un software di paghe di una nota azienda americana la *ADP US*.

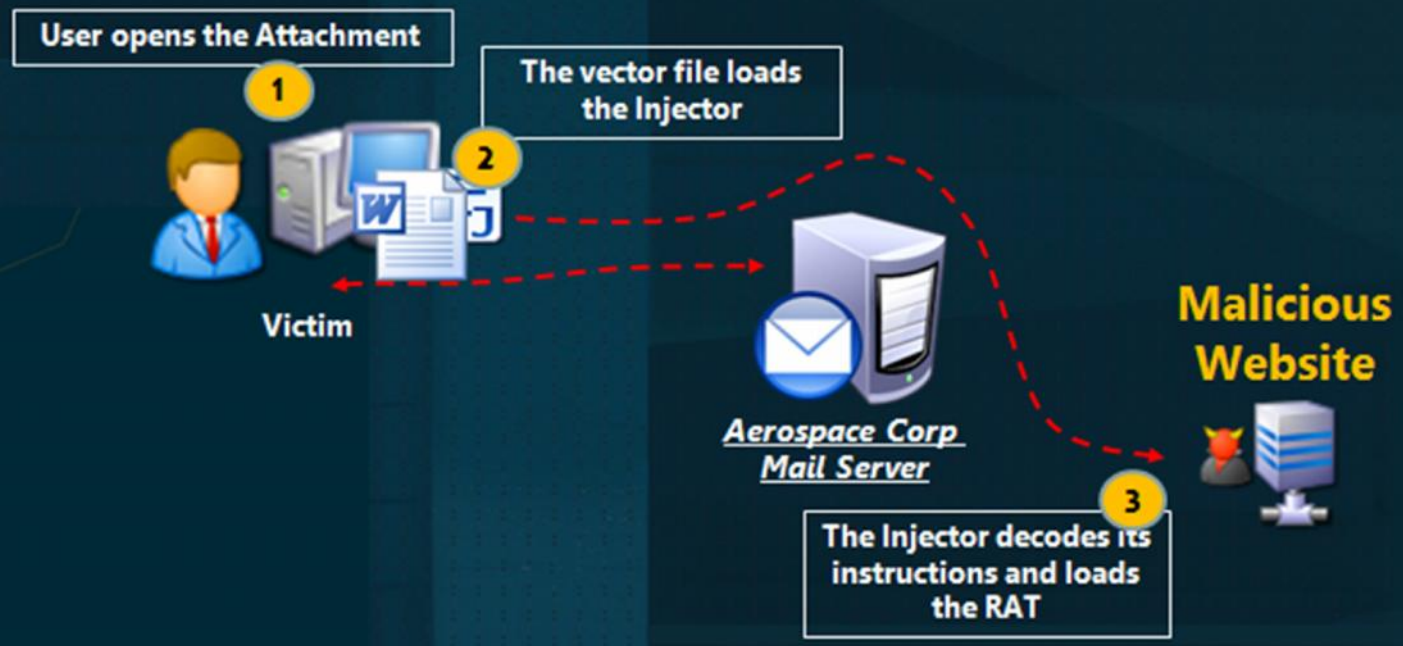


Boeing-job.com

- I messaggi iniettavano (Drive-By) due injector sviluppati ad-hoc per forzare le macchine vittima a caricare delle pagine di un dominio: www.boeing-job.com
- Questo dominio conteneva il secondo stadio dell'attacco:

id	os	browser	refer	ipaddress	flash	java	pv	visit_old	visit_new
10	Win 7	Firefox	http://www.boeing-job.com/jobs/?hl=en&tbo=d&output=upload&sclient=psy-ab&q=boeing&am	192.168.10.10	11.4.402.287	x	0	2013-01-22 18:59:41	2013-01-22 18:59:43
9	Win 7	Internet Explorer 8	http://www.boeing-job.com/jobs/?hl=en&tbo=d&output=upload&sclient=psy-ab&q=boeing&am	192.168.10.10	11.1.102.62	x	0	2013-01-22 13:21:25	2013-01-22 13:21:26
8	Win 7	Internet Explorer 8	http://www.boeing-job.com/jobs/?hl=en&tbo=d&output=upload&sclient=psy-ab&q=boeing&am	192.168.10.10	11.1.102.62	x	0	2013-01-22 13:21:25	2013-01-22 13:21:26
6	Win 7	Internet Explorer 8	http://www.boeing-job.com/jobs/?hl=en&tbo=d&output=upload&sclient=psy-ab&q=boeing&am	10.144.30.134	11.1.102.62	x	1	2013-01-22 12:13:18	2013-01-22 12:58:48
7	Win 7	Internet Explorer 8	http://www.boeing-job.com/jobs/?hl=en&tbo=d&output=upload&sclient=psy-ab&q=boeing&am	192.168.10.10	11.5.502.110	x	0	2013-01-22 12:52:41	2013-01-22 12:52:42
5	Win 7	Internet Explorer 8	http://www.boeing-job.com/jobs/?hl=en&tbo=d&output=upload&sclient=psy-ab&q=boeing&am	10.144.31.191	11.1.102.62	x	0	2013-01-22 11:30:17	2013-01-22 11:30:19
4	Win 7	Chrome	http://www.boeing-job.com/jobs/?hl=en&tbo=d&output=upload&sclient=psy-ab&q=boeing&am	192.168.10.10	11.531	x	1	2013-01-22 11:11:43	2013-01-22 11:23:58
2	Win Xp	Chrome	http://www.boeing-job.com/jobs/?aaa=aaa	192.168.10.10	11.531	x	3	2013-01-22 10:31:30	2013-01-22 10:52:03
3	Win Xp	Internet Explorer 8	http://www.boeing-job.com/jobs/	192.168.10.10	6.0.88.0	x	1	2013-01-22 10:46:59	2013-01-22 10:49:08
1	Win Xp	Chrome		192.168.10.10	NanFlash	NanJava	0	1969-12-31 21:00:00	2013-01-22 10:31:21

Attack Scheme



Attack Scheme

4 The RAT is installed

Victim

L'infezione iniettava un RAT customizzato, proveniente dal "ramo asiatico" di ProRAT e la sua C&C:

- ieee[.]boeing-job[.]com

5 The RAT communicates with its C&C

C&C

ieee[.]boeing-job[.]com

6 The attacker can spawn a Remote Shell on the Target or collect stolen data from the C&C

Remote Shell

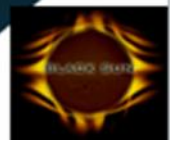
Attacker

Maggiori dettagli dell'attacco.

- Le macchine infettate puntavano quindi ad una C&C da cui i "controllori" potevano inviare comandi e trafugare dati, oppure potevano attivare una backdoor per accedere direttamente alla macchina target.
- *boeing-job[.]com* è stato registrato il 22 Gennaio 2013, su GoDaddy, con informazioni false.
- Il 5 Febbraio il suo sottodominio *http://ieee[.]boeing-job[.]com* puntava all'IP *108.62.10.13*, AS15003 negli USA.
  Il 6 Febbraio puntava all'IP *184.168.221.37*, AS26496 in USA, su GoDaddy.
- Ma se si tentava una ricerca da google *www.boeing-job[.]com*
- Si puntava a un dominio di primo livello legittimo:
  - *http://www[.]grupo-gestion[.]com[.]ar*,
  - con IP *200.123.160.138*, AS16814 sito in Argentina.
- Questo perché questa modalità di infezione era già stata usata a danno dei dipendenti della Boeing nel Gennaio 2013 con meccaniche simili.

ISACA
Rome Chapter

Attacchi Massivi Vs Attacchi Mirati: GONGDAD Exploit Kit



GONGDAD Exploit Kit

- Poco più di una settimana è passata da quando l'attacco alle aziende Aerospaziali è stato perpetrato e «guarda caso»… Gongdad, un noto exploit kit (parente stretto del più noto Kaixin) ha iniziato a sfruttare queste vulnerabilità all'interno del suo Injector.

```
else {

    if((NXBoB8['major']==11 && NXBoB8['minor']==4 && NXBoB8['rev']==402 && (NXBoB8['gondad']>= 265 && NXBoB8['gondad']<
        = 287)) || (NXBoB8['major']==11 && NXBoB8['minor']==5 && NXBoB8['rev']==502 && (NXBoB8['gondad']>= 110 &&
        NXBoB8['gondad']<= 146))){

    document.writeln("<img src=myrF03.swf><\/img>");
    setTimeout("document.writeln(\"<embed width=100 height=0 src=myrF03.swf><\\/embed>\");",2000);
    }
```

```
public class ByteArrayAsset extends flash.utils.ByteArray implements mx.core.IFlexAsset
{
    public function ByteArrayAsset()
```

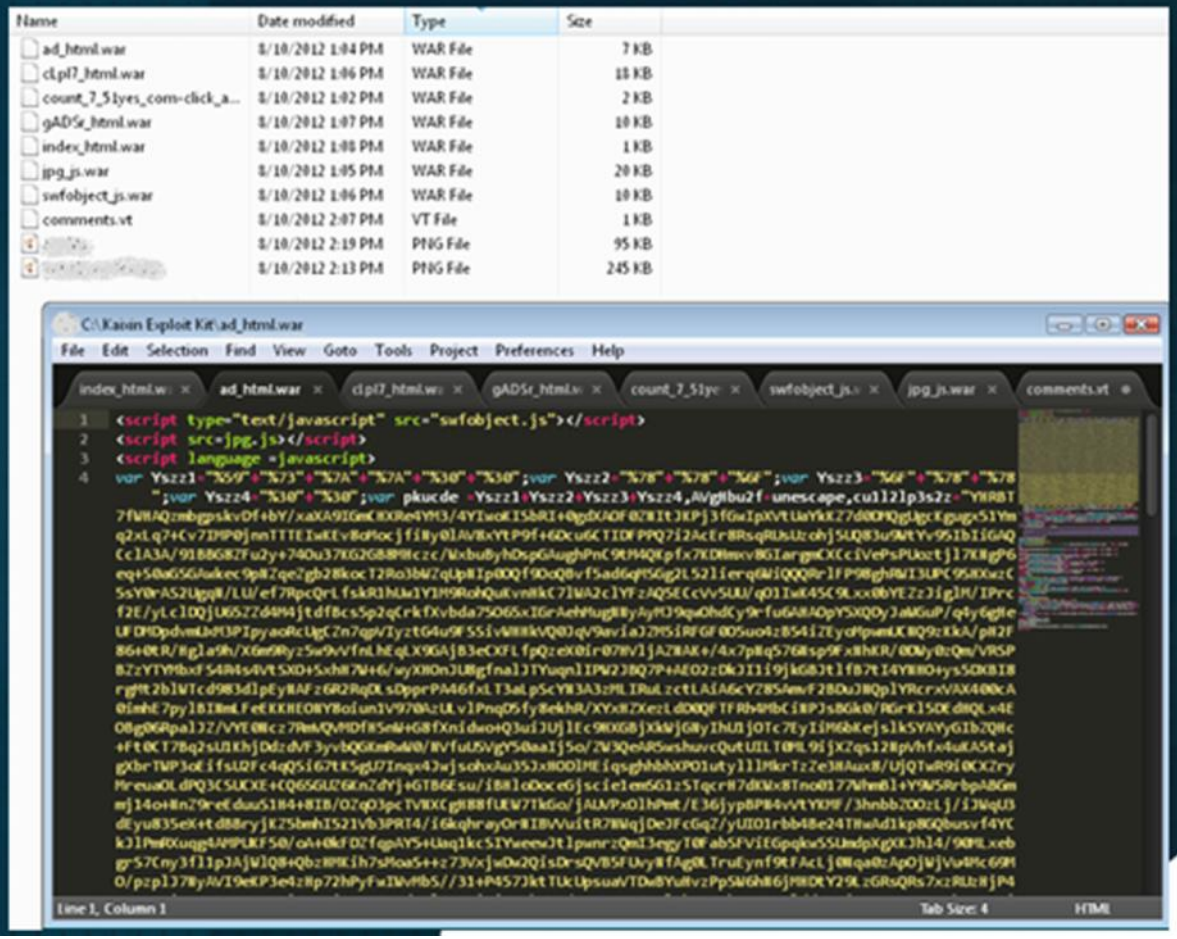
```
public class LadyBoyle extends flash.display.Sprite
{
    public function LadyBoyle()
    {
        var loc1:*=null;
```

GONGDAD Exploit Kit

- Dal momento della pubblicazione dell'attacco via file word e dell'identificazione delle due vulnerabilità abbiamo attivato, in collaborazione con gli altri enti di ricerca, una serie di regole di ispezione sul traffico. Il 23 Febbraio magicamente scopriamo questo sito: *"http://www.jhtyhtrsgr.com/yymex/index.html"* all'IP 69.197.61.29, negli USA, registrato il 22 Febbraio 2013 con informazioni false
  - Admin: *"jing yan (ttfu7ii777@126.com) –*
  - *Registar: GuangMing yanjing".*
- L'*"index.html"* di questo sito contiene un Injector in JavaScript *"JSXX VIP JS Obfuscator".*
- Dopo l'iniezione dell'Injector contenuto nel file *"index.html"* il redirect porta la vittima a subire l'infezione dell'Exploit Kit: Gong Da.

GONGDAD Exploit Kit: origini

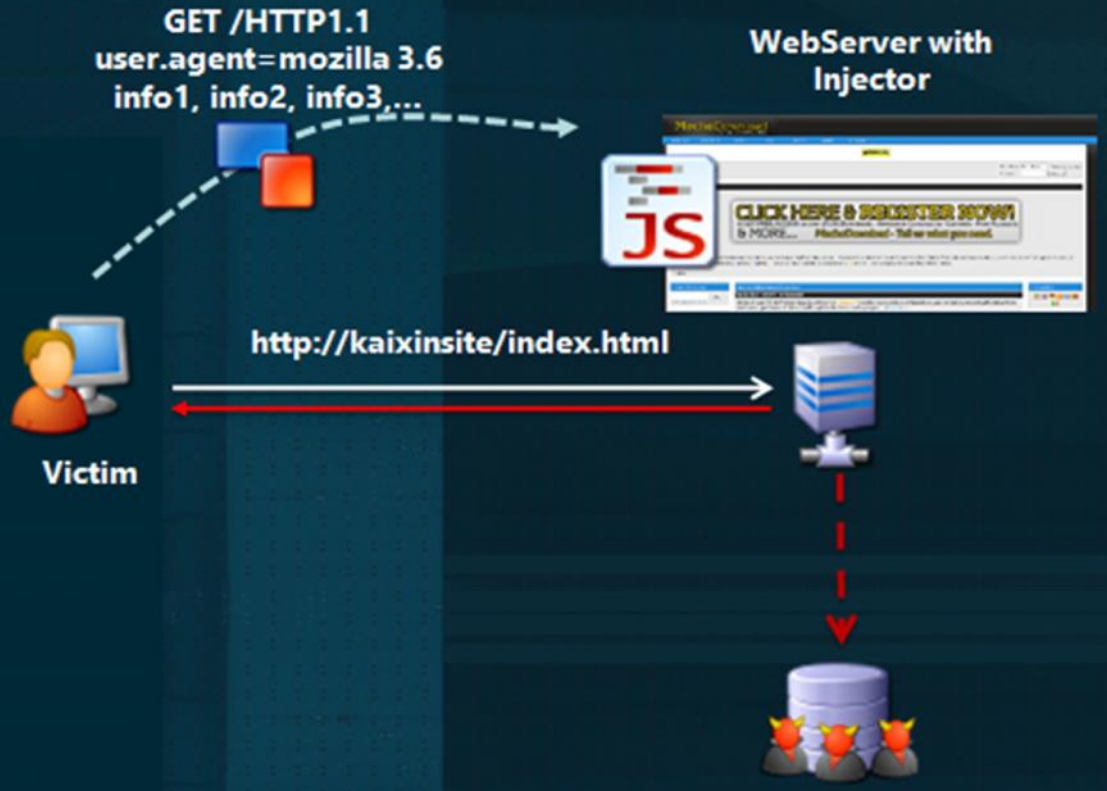
- Ma Gongdad non nasce dal nulla.
- Il suo precursore e padre è il ben noto Kaixin, un Exploit Kit ancora attivo.



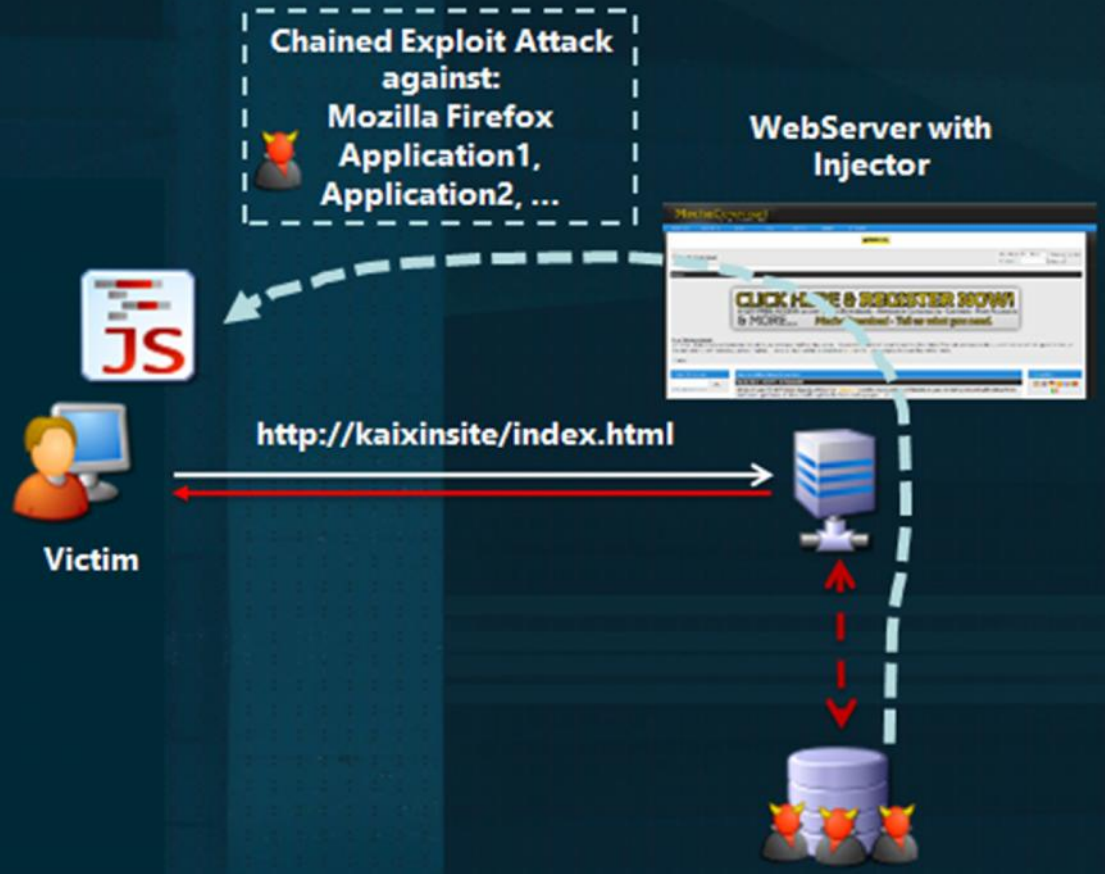
KAIXIN EK

- CVE-2011-3544 : Una vulnerabilità Java.
- CVE-2012-0507 : Un'altra vulnerabilità Java.
- CVE-2012-1723 : Una terza vulnerabilità Java.
- CVE-2012-0754 : Una vulnerabilità Adobe Reader.
- CVE-2012-1889 : Una vulnerabilità al Servizio XML Core dei Sistemi Microsoft.
- Ad Agosto KaiXin ha visto sostituite alcune delle sue vulnerabilità, ovvero Java **CVE-2012-0507** e **CVE-2012-0754** con nuove vulnerabilità:
  - Java CVE-2012-1723
  - Java CVE-2012-4681
  - Java CVE-2012-5076 .
- In buona sostanza queste vulnerabilità sono state identificate, con la stessa progressione anche nell'Exploit Kit GONGDAD

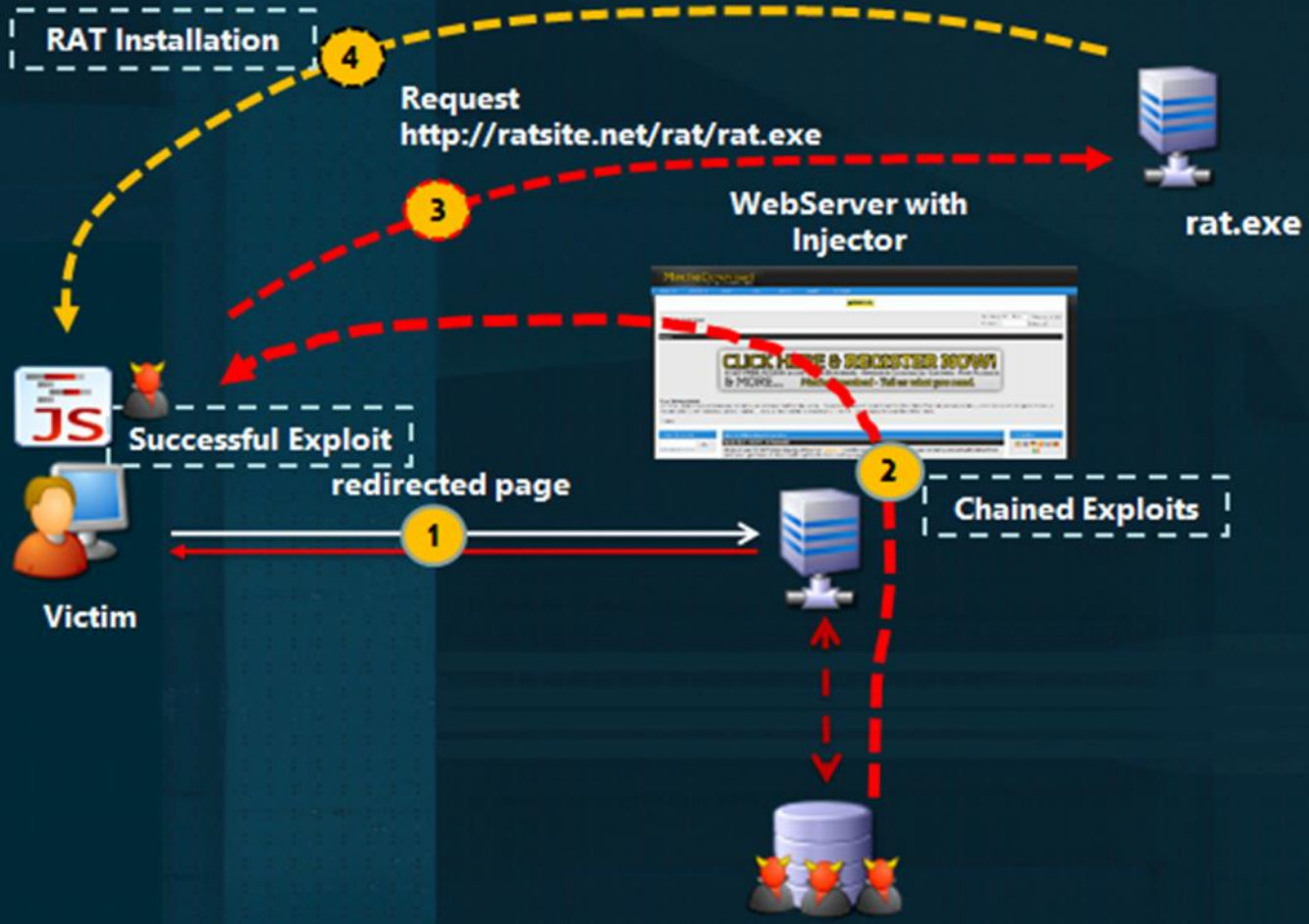
Le meccaniche di attacco



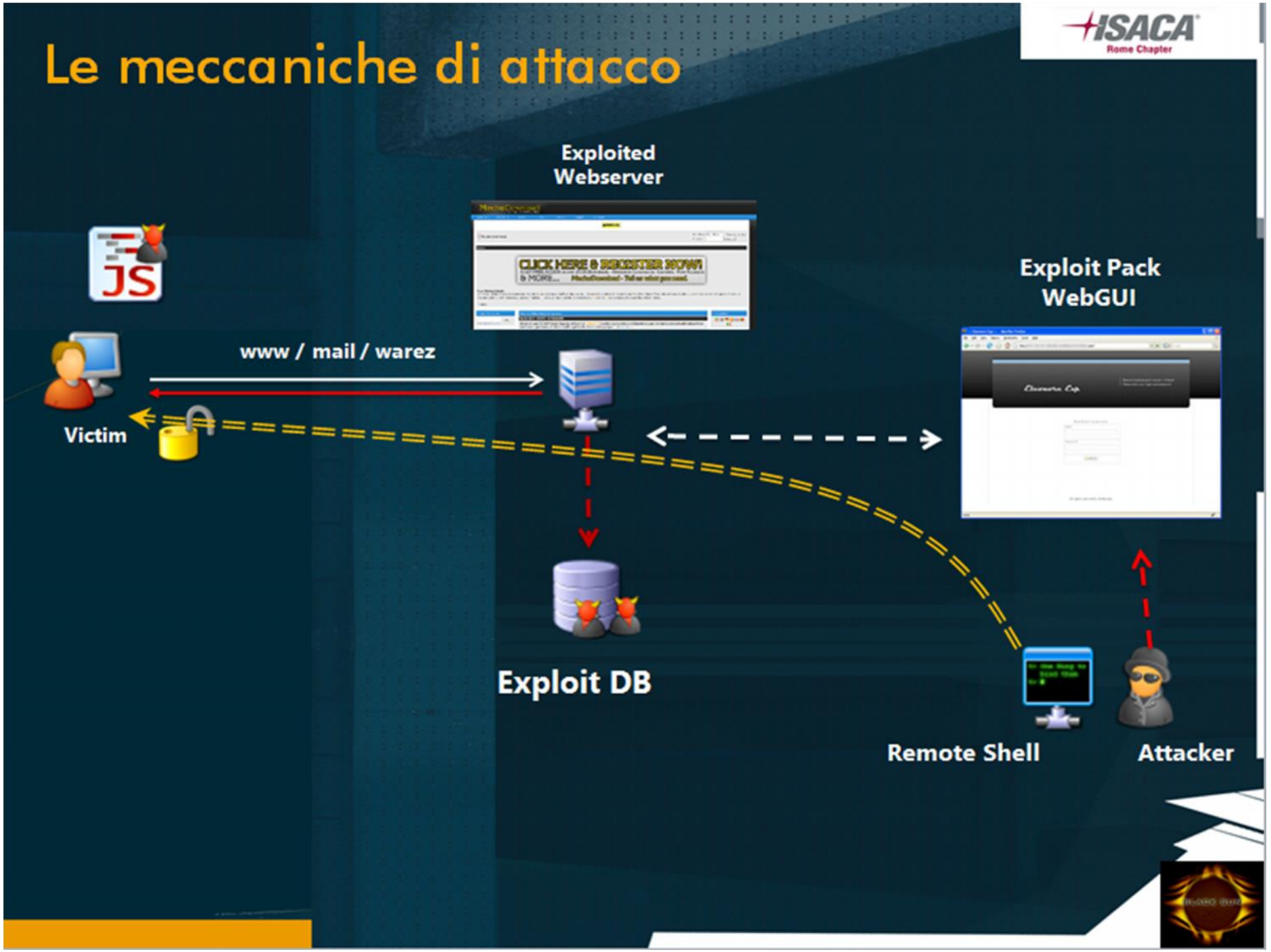
Le meccaniche di attacco



Le meccaniche di attacco



Le meccaniche di attacco



Soluzioni rapide? No way…

- Le strategie di mitigazione che sono implementate dalle componenti di rete, quali firewall, router o proxy, sono facilmente eludibili per mezzo di contenuti offuscati o criptati.
- Le tecniche di white/black listing soffrono delle latenze che ne impediscono un reale utilizzo in modo puntuale.
- Poiché i nuovi attacchi hanno come obiettivo gli applicativi (quali il browser e le sue componenti), e mancando oggi dei meccanismi di difesa integrata la problematica è oggi fonte di grandi preoccupazioni.
- È quindi necessario elaborare differenti strategie di mitigazione.

Le azioni mitigatrici

- Per aiutare nella mitigazione è essenziale ricorrere all'ausilio non solo delle tecnologie, ma anche delle informazioni utili a identificare preventivamente le fonti degli attacchi di tipo «Drive-By».
- Per questo l'esperienza ci ha insegnato che:
  - L'Early Warning
  - L'intelligence
  - L'IP Reputation
  - Gli IPS/IDS
- Sono le principali fonti da cui trarre le indicazioni per predisporre una adeguata e funzionale barriera a queste minacce.

L'analisi di un incidente da Exploit Pack

- A seguito dell'identificazione di un incidente prodotto o promosso da «Drive-by» è poi essenziale comprendere le meccaniche di manifestazione dello stesso per poterne inferire le possibili procedure e azioni per la riduzione del rischio, elemento questo che porta il CERT o il SOC a dover «ripercorrere» logicamente, il path dell'infezione (quando possibile).
- In questi casi si consiglia di procedere con un'analisi di laboratorio o di ricorrere all'ausilio di personale esperto in malware analysis e/o criptovirologia, considerando che nella maggior parte dei casi i contenuti maliziosi si presentano (quando ancora persistenti nel terminale) in modalità crittografata.

L'Incident Response

- La situazione "reattiva" più frequente è l'identificazione di una vittima a seguito della sua compromissione, quando l'injector del Drive-by evolve nell'installazione di un RAT (Remote Access Trojan) o in uno Stealer.
- Questi malware possono attivare maggiori segnali all'interno della rete e dei Sistemi.
- Il problema, in questi casi, è che la "reazione" comporta una mitigazione su quest'ultimo aspetto, ovvero sul più tradizionale malware e meno probabilmente sul vettore che l'ha depositato all'interno della struttura di rete e che ha permesso la prima compromissione.

L'analisi di un incidente da Exploit Pack

1. Analisi dei Log via IPS/IDS
2. Analisi via Network Analyzer
3. Analisi dell'injector via Sandbox
4. Binary decode dell'injector
5. C&C Hunting (post infezione)

ISACA
Rome Chapter

Grazie per l'attenzione

Stefano Maccaglia
Chief Research Officer
Black Sun Labs

26 Marzo 2013