Scheda informativa sul security service challenge 6 (ssc6)

Cos'e' il security service challenge

Il security service challenge è una simulazione di un incidente di sicurezza che viene eseguito con l'intento di analizzare la capacità di risposta di siti, NGI e EGI CSIRT sulla base della procedura ufficiale EGI .

Tutte le informazioni trovate nelle varie indagini dovranno essere riportate sulla base del modello previsto dalla porcedura stessa.

Scenario: uso improprio di credenziali grid rubate

Poichè l'uso improprio di credenziali grid rubate rappresenta una potenziale minaccia per l'intera infrastruttura, lo scenario che si è pensato di usare è appunto quello di un job autenticato ed autorizzato ad essere eseguito sui worker nodes di un sito grid. I siti avranno dunque a che fare con un certificato x509 di un utente usato per generare delle credenziali grid al fine di eseguire dei job che simuleranno le tipiche attività di un malware.

Come verranno notificati i siti

Durante la simulazione il sistema di ticketing RT verrà usato per comunicare con i siti. Per ognuno di questi verrà dunque aperto un ticket che invierà una mail alla lista di sicurezza (`CSIRT E-Mail` nel GOCDB) dei siti coinvolti. Tale mail conterrà delle informazioni generali ed altre più specifiche relative al presunto incidente (es. DN coinvolto). Per rispondere al ticekt è sufficiente rispondere alla mail.

Si prega di notare che il mittente della mail sarà: Giuseppe Misurelli via RT <ssc-monitor@raaf.nikhefhousing.nl>

Cosa ci si aspetta dai siti coinvolti

Il sito coinvolto nella simulazione dovrà comportarsi come se si trattasse di un normale incidente con le seguenti eccezioni:

1. **Nessuna sanzione (es. esclusione anche temporanea) della VO coinvolta**
2. **Tutte le comunicazioni devono essere inviate in maniera esclusiva all'apposito indirizzo mail predisposto (si prega di non usare `abuse(at)egi.eu`)**

Le informazioni più rilevanti ai fini della risoluzione dell'incidente possono essere riassunte nelle seguenti domande

Rete

- Nel WN in cui i job sono in esecuzione vi sono delle connessioni aperte sospette? Se si verso quali IP?
- Il sito si avvale di un servizio (es. netflow) che possa mettere in evidenza connessioni di questo tipo?

Contenimento

- Il processo riconducibile al "malware" appartiene ad un batch job o ad una shell interattiva?
- Da dove è stato eseguito il job (WMS e/o UI)? Avvalersi dell'ausilio della NGI che gestisce i WMS chiedendo informazioni a grid-operationslists.infn.it (specificare l'attività SSC6)
- Da quanto tempo il job è in esecuzione (es. YYYY:MM:DD hh:mm)?
- Come posso fare per escludere il DN?

Analisi malware

- Si riesce a trovare il malware e a capirne le funzionalità?

Utilità per i siti

Lista di pratiche, procedure e setup utili ai siti nello svolgimento della simulazione.

Service reference card dei servizi grid coinvolti

- Computing element
- Worker node

Esclusione centralizzata del DN coinvolto

Durante la simulazione è possibile provare la funzionalità di "central banning" operata dalla NGI. Dopo aver concordato la cosa fra NGI e siti coinvolti, alcune configurazioni si rendono necessarie nei siti. Tali configurazioni differiscono a seconda dell'uso o meno del servizio Argus come sistema di autenticazione per i job grid.

Per ulteriori informazioni fare riferimento alla guida Central banning setup for sites .

Approccio sommario ma veloce all'analisi forense

Informazioni utli ad un'analisi "quick and dirty" possono essere trovate nella presentazione fatta da un esperto di EGI CSIRT allo scorso forum tecnico EGI (allegata in calce). Un modo di procedere molto semplice e immediato per la raccolta di informazioni utili viene descritto unitamente ad uno script python capace di "ripulire" i timestamps presi presentandoli in modo più intuitivo per la lettura di eventi riconducibili all'attività sospetta.

Esempio raccolta timestamps per l'intero fiesystem:

```
find / -xdev -print0 | xargs -0 stat -c "%Y %X %Z %A %U %G %n" >
timestamps.dat

timeline-decorator.py < timestamps.dat | sort -n > timeline.txt
```
(timeline-decorator.py in calce)

Spunti di discussione con i siti coinvolti nella simulazione

- Data/orario di inizio
  - ♦ A seconda della disponibilità decidere se fare tutti i siti in un'unica soluzione o dividerli
- VO usata (infngrid) e compatibilità con le varie policy di MaxCPU/WallTime
  - ♦ Limitazioni con la durata del proxy (24h) e quella del job in esecuzione sulla coda cert
  - ♦ VO alternative non su coda cert? (Es. gridit)
- Test di comunicazione fra il coordinamento dell'incidente (NGI_IT) ed i contatti di sicurezza dei siti coinvolti
  - ♦ Via ticket rt (mail alla vostra lista grid-sec)
- Esempi pratici di estrazione di "timestamps" come indicati nel pdf allegato
  - ♦ Possono essere d'ausilio ai siti?
- Uso del "central banning"
  - ♦ Attività di configurazioni richieste per l'integrazione dei CE coinvolti nel sistema centrale

This topic: SiteAdminCorner > NGI_ITSSC6
Topic revision: r7 - 2013-11-21 - GiuseppeMisurelli