PV210 Bezpečnostní analýza síťového provozu

Úvod do forenzní analýzy

Michal Procházka, Daniel Kouřil

3. 12. 2014

Řešení domácího úkolu, shrnutí z minula

Kontext, cíle, zasazení do životního cyklu incidentu

Sběr dat pro forenzní analýzu

Zpracování dat, analýza, manipulace s daty

Reportování z forenzní analýzy

Řešení třetího domácího úkolu I

Hlášení č. 1 – phishing bez hlaviček

- Phishingová stránka běží na `http://webmastersecurehelpdeskadmincz1.jimdo.com`
- Útočník využívá webhosting Jimdo (`http://www.jimdo.com`)
- Whois pro `jimdo.com` vrací `support@jimdo.com`.
- Alternativní řešení: překlad jména stroje na IP (69.174.241.32) a následně whois vrátí `abuse@serverbeach.com`.

Řešení třetího domácího úkolu II

Hlášení č. 2 – phishing s hlavičkami

- Stránka běží na `http://www.trustworthyseal.com/app/forms/form1.html`.
- Pravděpodobně jde o zneužití firemní prezentace (liší se od hlášení č. 1).
- Překlad jména na IP (192.185.5.192) a následně whois vrátí `ipadmin@websitewelcome.com`.
- Alternativní řešení: návštěva `http://websitewelcome.com/` a odtud `abuse@websitewelcome.com`.

Řešení třetího domácího úkolu III

- Webmail: z *první* hlavičky vezmeme `webmail.med.uoc.gr` (ujistí nás Google s dotazem "Horde Framework").
- Překlad jména na IP (147.52.72.199).
- Whois na Domaintools vrátí několik e-mailů, z nichž vezmeme ty v polích e-mail (ne changed):

  `mstarvak@ucnet.uoc.gr, jfragiad@ucnet.uoc.gr, kalogirou@ucnet.uoc.gr.`
- Whois v Linuxu nevrátí žádné e-maily. Nutno hledat na webu Krétské univerzity.
- Stroj patří Krétské univerzitě a ta by možná mohla spadat pod akademický tým GRNET-CERT.
- Zcela jistě ale spadá pod národní tým NCERT-GR (dle záznamu u Trusted Introducera).

Řešení třetího domácího úkolu IV

- Hodnocení se objeví v Poznámkovém bloku do přednášky 10. 12.
- Hodnocení: 0–10 bodů. Viz zadání projektu (interaktivní osnova).
- Kontaktní osobou pro tento úkol je Jan Vykopal.

Shrnutí minulé přednášky

- CSIRT týmy poskytují část služeb, která nejlépe vyhovuje konstituency
- Nejzásadejnější je IH, pak jsou další služby
- Různé úrovně a podoby IH, převážně dle typu organizace

Tradiční vs. digitální forenzní analýza

Příklad incidentu

- Provedení
- Zjištěná fakta
- Možné dotazy
  - Známe vstupní vektor?
  - Byla modifikována data?
  - Lze dohledat útočníka (GPS, FB)?

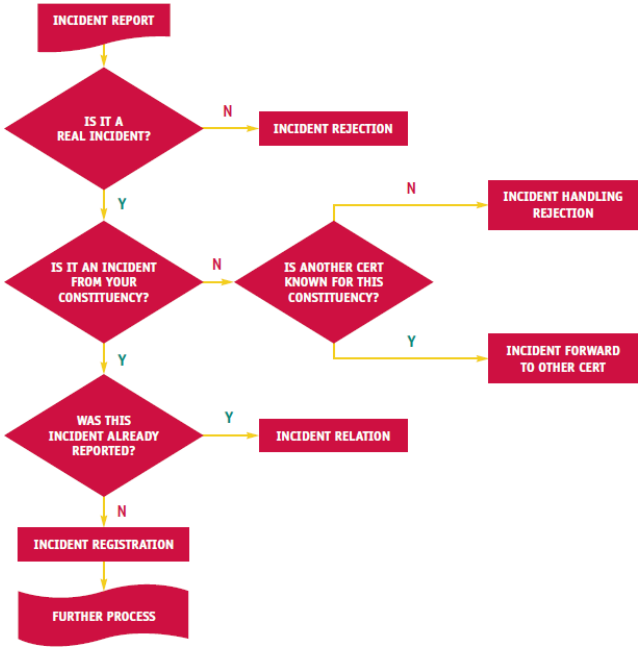
např. Neautorizovaný přístup ke sdílenému disku ve Windows doméně a zkopírování, smazání citlivých dat.

Řešení incidentu

- Řešení bez FA
  - Detekce
  - Informování
  - Uvedení do původního stavu
- Řešení s FA
  - Detekce
  - Informování
  - Analýza (uvedení do původního stavu)
  - Zpětná vazba
  - Uvedení do původního stavu

Životní cyklus incidentu

- Pokračování “Further Process”
- Postup alá NIST
  - (Preparation)
  - Detection and Analysis
  - Containment, Eradication, Recovery
  - Post-Incident Activity



- Prvky FA součástí třech posledních fází

  `http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf`

Incident handling – zopakování

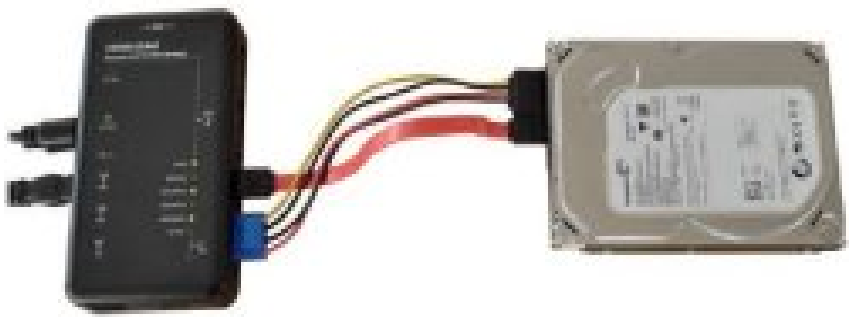
- Analýza incidentu
- Řešení incidentu na místě
- Podpora řešení incidentu
- Koordinace řešení incidentu

Forenzní analýza

- Zjištění příčin útoku, vstupní vektor
  - Sběr a vyhodnocení dostupných informací
  - Dohledání dat, modifikovaných a smazaných souborů
- Kategorizace závažnosti
- Uchování důkazů
- Co je vysledkem FA? Vždy je nutné **zadáni**!
  - Příklady (RAC, govCERT, “koncový” CSIRT)
- `http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf`

Fáze forenzní analýzy

1. Sběr primárních dat
2. Vyhodnocení, analýza
3. Reporting



Týmová spolupráce

- Role
  - Techničtí experti
  - Právníci
  - Koordinátor
  - Komunikace s médi
  - Komunikace s jinými CSIRT týmy
  - Vedení firmy
- Sdílení i předběžných výsledků (lze-li)
- Pozor na legislativní omezení
  - Orchana osobních údajů
  - Klasifikace utajení (státní správa)

Základní principy

- Detailní poznámky během získávání dat
  - Obhajitelnost i po letech
  - Práce minimálně ve dvojici
  - Fotodokumentace, video záznam
- Vždy v souladu s lokálními předpisy a legislativou
  - Ochrana osobních údajů
  - Firemní předpisy
- Minimální změny ve zkoumaných systémech
- Check-list a školení předem
- No panic!

Sběr dat

Podle úrovně volatility (RFC 3227), zjednodušeně:

- Síťové konfigurace (spojení, ARP, . . .), procesy, paměť
- Pevné disky, paměťové karty - filesystem
- Externí logy, síťový monitoring
- Dodatečné netechnické zdroje (sociální sítě, “výpovědi” uživatelů, kamerové a docházkové systémy, . . .)

Sběr dat

- Příklady
  - časová razítka - z disku
  - paměť procesů - z RAM, hesla, klíče
  - síťová spojení - spojení na C&C
  - flow
  - logy systému a aplikací
- Nikdy se předem neví, co bude potřeba
- Možnosti sběru závisí podle důležitosti služby (její dostupnost)

Zpracování dat

- Na zpracování je více času
- Lze provádět opakovaně
- Analýzy provádět v uzavřeném prostředí
- Opět záleží na zadání
  - Probíhající incident: rychlá analýza, odhalení cíle, . . .
  - Obnovení dat: může trvat déle
- Týmová spolupráce
- Budování teorie
- Automatizace

Ochrana primárních dat

- Aplikovat už během sběru dat
  - Podle závažnosti (pro potřeby Policie)
  - Fotografie, videozáznamy, dokumentace, protokoly
- Manipulace - chain of custody

Typy

- Zpráva o průběhu FA
  - Detailní, ověřitelné informace
  - Pouze má-li smysl
- Zpráva s výsledky
  - předběžná
  - průběžná
  - závěrečná

Průběžná komunikace

- Informování vedení firmy, dotčených stran, získání dalších podkladů
- TLP - (Traffic Light Protocol)
  - Red - Pouze v rámci skupiny
  - Amber - Pouze v rámci organizace
  - Green - S partnery
  - White - Veřejně

Reportování výsledků

- Jasná odpověď na zadané otázky
- V případě obecného řešení incidentů
  - Informace užitečné pro ostatní (základ pro advisory)
  - Informace o možných síťových vzorech
  - Doporučení pro nápravu

Ukázkový report

```
Summary
-------
A machine running on FEDCLOUD-SITE  was detected to initiate ddos ddos
against victims on the Internet. Analysis of the machine showed
malware injected via an insufficiently secured Tomcat instance, which
was used by the attacker to launch malicious activities from the node.
The virtual machine was isolated soon after the findings and its owners
notified. The corresponding image was found to contain the vulnerable
configuration and was removed from EGI AppDB.

Hosts involved
--------------
The machine attacked was running with aa.bb.cc.dd, the attacker used
C&C at  aa.bb.cc.dd (25000/tcp). The identified ddos attack targeted at
three IPs, aa.bb.cc.dd, aa.bb.cc.dd, aa.bb.cc.dd

Evidence of compromise
----------------------
The malware was running as process Confg, which has TCP connection open
to the C&C (aa.bb.cc.dd). The binary of the process was stored as
/tmp/Confg and owned by the tomcat7 user.

DDoS attacks targeted ports 53/udp, no attempt to amplify the traffic or
spoof source IP addresses was detected. The activity was therefore easy
to trace on the network level. The maximum volume of the attack was at
rate of 50 thousands UDP packets per second.

Details of the attack
---------------------
The attack vector used was Tomcat with the Manager servlet enabled with
default credentials "admin:admin". This common vulnerability is a target
of frequent scans on the Internet. We have no reasons to believe the attacker
targetted specifically EGI resources. It is very likely the machine was
actually attacked by three independent attacks.

The attack triggering the ddos floods used a malicious process which was
instructed by the attackers' C&C. The corresponding binary is based on
the Bill Gates trojan family (see e.g.
http://securelist.com/analysis/publications/64361/versatile-ddos-trojan-for-linux)

Possible vulnerabilities exploited by attacker
----------------------------------------------
Unsecure configuration of Tomcat

Actions taken to resolve the incident
-------------------------------------
Analysis of the incident showed that the vulnerability was present in
the image used to instantiate the virtual machine. Sites where the image
was in use were detected and asked to remove the image and investiage virtual
machines running off the image. The owner of the image was also notified
and the image was removed from the EGI AppDb repository. The related
contents was available as:
  https://appdb.egi.eu/store/vappliance/guse.proxy.dci.bridge
  https://appdb.egi.eu/store/software/fedcloud.slave.dci.bridge

Additional discussions about incident handling will carry on in the
FedCloud community.

Timeline of the incident
------------------------
15-16. Oct - DDos attacks performed from the node
22. Oct - attacks detected by the CESNET security teams
24. Oct - verification of the incident, notification of EGI CSIRT, suspension of the VM
25. Oct - initial report sent to the fedcloud sites and mgmt, removal of the vulnerable image
```

Shrnutí

- FA součást IH, v různých fázích
  - značně expertní činnost, lze outsourcovat
- Tři základní fáze
- Opatrnost při sběru dat a při jejich uchování
  - zejména hrozí-li právní spory
- Vedle technických aspektů je důležitá i komunikace a reporting, a koordinace

Další materiály

- SANS - http://sans.org
- Forensics Wiki - http://forensicswiki.org
- Sleuth Kit - http://www.sleuthkit.org