Lessons Learned from TLD Incidents

Based on tld-ir-checklist-01sep15-en.pdf

Using Lessons Learned from TLD Incidents as a Guide

- TLD Incident Response Checklist was developed in response to recent incidents.
- Covers technical, legal, and media considerations
- Lets use this fresh knowledge as a guide to secure registry operations

Investigation Basics

- Was the system *really* compromised?
- What was the path of entry?
- What did the attackers do while they had unauthorized access? Specifically, what has been altered? Deleted? Disclosed?
- What traces did the attackers leave that I can use to identify the (criminal) actor?
- How should I recover from the compromise?
- What are my reporting (disclosure) obligations?

Follow your Incident Response plan

- What? Don’t have one? Notify Exec, Legal, and Spokesperson
- Legal action? Considered criminal? Then IT system is a “crime scene”. Treat it that way.
  - Preserve evidence
  - Do not turn systems off before backup
  - May need outside professional forensic expertise

Preserve the (crime?) scene

1. Do not turn off until disk and RAM copied.
2. Disconnect the compromised system from the network and put spares into service ensuring they are not vulnerable to same attack.
3. Immediately make at least two image copies of the system's disks. Protect chain of custody for this “evidence”.
4. Prepare to build clean, new system(s) dedicated to hosting the authoritative name service. Do NOT SHARE SERVERS! E.g., attack via Web applications is the most common attack vector.

Investigating the servers

- Review file system to identify any file system changes (Tripwire?). Look for unfamiliar/unauthorized directories user accounts, unfamiliar privileges granted to familiar user accounts, and for process accounting or log information (lastcomm?). Any unauthorized secure shell (ssh) preshared keys, or unexpected setUID/setGID binaries?
- Review log files to identify unusual account, processes, services (especially listeners) and communications activities.
- Review zone file data. Compare against the last known-to-be-correct zone
- If an external party reported the compromise, how did they determine the name server was compromised?
- Document findings

Restore Auth Name Server O/S

- Erase drive, install O/S, patch, overwrite BIOS.
- Create new root/admin accounts with good passwords. Limit access to only DNS admin and system access from limited set of IP addresses
- Enable unattended security updates
- Setup Secure Shell for encrypted remote access using keys.
- Reduce the attack service by disabling all non-essential services.
- Set up system monitoring (swatch?, tripwire?, iptables?)
- Enable process accounting (acct?)
- Consider implementing currently available Linux security extensions.
- Use/build dedicated log server and configure remote syslog.

Restore Auth Name Server

- Install your DNS server software, patch, and configure nameserver logging.
- Do not copy any files from the compromised system over to a new server. Prior backups from uncompromised system are ok.
- Configure DNS server as authoritative
- Disable recursion
- Prepare zone data on another system maintained externally which uploads to this one (hidden master).
- Enable checks to verify zone integrity.
- Run Network Time Protocol (NTP)
- Arrange external monitoring of server integrity, consistency of records in root and TLD and WHOIS (e.g., NS)
- Again - Compartmentalize DNS, mail, www, etc… Separate machines and networks!!
- Backup configuration files and document above steps as part of IR plan.

Recover and Restore other services

- If you must leave compromised system up (e.g., legal authorities insist)
  - Add countermeasures to ensure that the attacker cannot disable remote logging or extend his attack to other systems or networks.
  - Add measures to block any malicious traffic that the attacker may attempt to generate from the compromised system.
  - Consider putting in place honeypots, canary accounts, or other methods to track future activities of the attacker.
- Install affected services on the new application servers on segregated LAN segments – patching and hardening where applicable.
- Synchronize time (use NTP).
- Enable remote logging.
- Generate new digital certificates for secure services such as HTTPS.
- Configure user accounts. Enforce a strong password policy by implementing password complexity.
- Notify authorized users of the event, provide instructions for remedial actions they should take.